Cloud Bastion Host

Best Practices

Issue	03
Date	2024-09-19

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Change CBH Instance Specifications

1.1 Before You Start

Application Scenarios

You can change specifications of a CBH instance to meet your business needs.

This document applies to specification changes of a single-node CBH instance on Huawei Cloud.

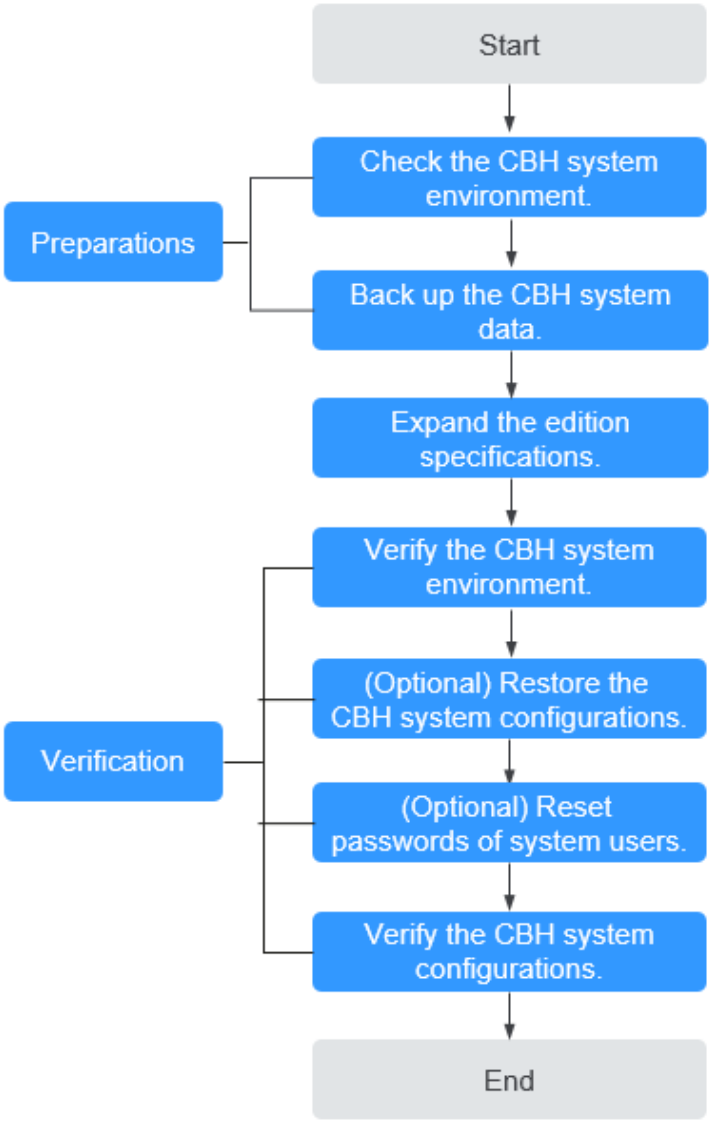
NOTE

To change specifications of a CBH instance in two-node cluster mode, click **Service Tickets** in the Huawei Cloud management console and submit a service ticket for technical support.

Change Process

This document provides guidance for the system administrator **admin** to change specifications of a CBH instance. The general steps are as follows: Back up the CBH system data before the change; change the instance specifications; restore the CBH system configurations; and verify that the configurations for the original and new CBH systems are consistent.

Figure 1-1 Specification change process



Restrictions on Changing Specifications

Changing specification includes changing the edition and asset specifications of a CBH instance.

- Edition: The edition of a CBH instance can only be changed from the standard to the professional, but cannot be changed from the professional to the standard.
- Asset specifications: include assets, concurrent requests, CPU, memory, and data disks. Asset specifications can only be scaled up.

NOTE

- Changing specifications has no impact on the bandwidth and traffic of the EIP bound to the instance.
- The default capacity of the system disk is 100 GB. Changing specifications does not affect the system disk but expands data disk capacity.
- CBH historical edition provides only functions of the standard edition. To change its specifications, click **Service Tickets** in the upper right corner of the Huawei Cloud management console and submit a service ticket for technical support.
- Change rules:

  Standard edition: A standard edition can be changed to another standard edition as long as the new one has a larger asset quota than the original. A standard edition can also be changed to a professional edition as long as the professional edition has an asset quota no less than the original edition does.

  Professional edition: A professional edition can be changed to another professional edition as long as the new one has a larger asset quota than the original.

Table 1-1 Edition change

Before the Change	After the Change
50 Assets | Standard	50 Assets | Professional 100 Assets | Standard or Professional 200 Assets | Standard or Professional 500 Assets | Standard or Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
50 Assets | Professional	100 Assets | Professional 200 Assets | Professional 500 Assets | Professional 1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
100 Assets | Standard	100 Assets | Professional 200 Assets | Standard or Professional 500 Assets | Standard or Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional

Before the Change	After the Change
100 Assets | Professional	200 Assets | Professional 500 Assets | Professional 1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
200 Assets | Standard	200 Assets | Professional 500 Assets | Standard or Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
200 Assets | Professional	500 Assets | Professional 1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
500 Assets | Standard	500 Assets | Professional 1000 Assets | Standard or Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
500 Assets | Professional	1000 Assets | Professional 2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
1000 Assets | Standard	1000 Assets | Professional 2000 Assets | Standard or Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional
1000 Assets | Professional	2000 Assets | Professional 5000 Assets | Professional 10,000 Assets | Professional
2000 Assets | Standard	2000 Assets | Professional 5000 Assets | Standard or Professional 10,000 Assets | Standard or Professional

Before the Change	After the Change
2000 Assets | Professional	5000 Assets | Professional 10,000 Assets | Professional
5000 Assets | Standard	5000 Assets | Professional 10,000 Assets | Standard or Professional
5000 Assets | Professional	10,000 Assets | Professional

Precautions for Changing Specifications

- **Software version**

  To make the functions of the profession edition take effect, the CBH system software version must be V3.2.16.0 or later, or the CBH system cannot be upgraded even the specifications are changed.

  If the software version is earlier than V3.2.16.0, **upgrade the system version** first.

- **System data backup and restoration**

  Before you change specifications, back up important system data to prevent system data loss caused by change failures.

  After the specifications are changed, reload the backup data to the system to quickly restore the system configurations.

- **Specification change time**

  The entire specification change process includes preparation, background upgrade, and verification after the change. The process takes about 60 minutes. It takes about 30 minutes to change the backend specifications. During this period, close the CBH system, which will interrupt the CBH system service.

  To reduce the impact on the system running, change specifications during off-peak hours.

1.2 Preparations

1.2.1 Checking the System Environment

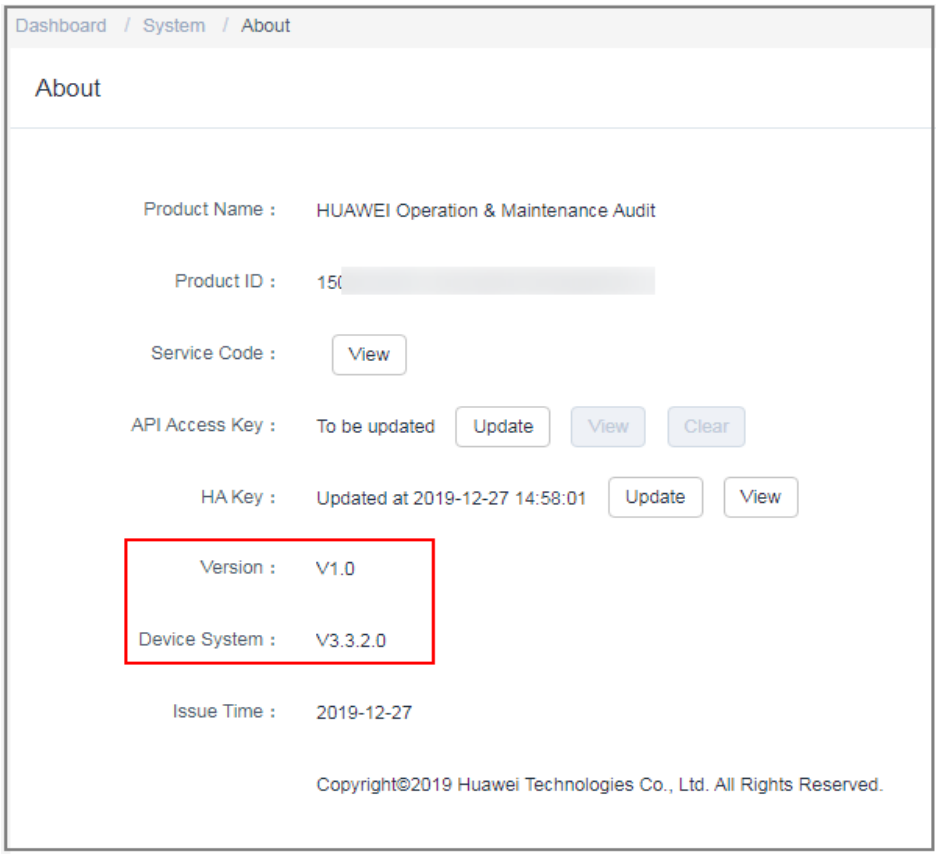
Before the change, query and record the system version information and specifications, including **Version**, **Device System**, **Max Resources**, and **Max Concurrent Conns**.

Step 1 Log in to the CBH system.

Step 2 Confirm and record the version number of the CBH system.

1. In the navigation pane on the left, choose **System** > **About** to view the system version information.

Figure 1-2 Viewing CBH system version number



2. Record information about **Version** and **Device System**.

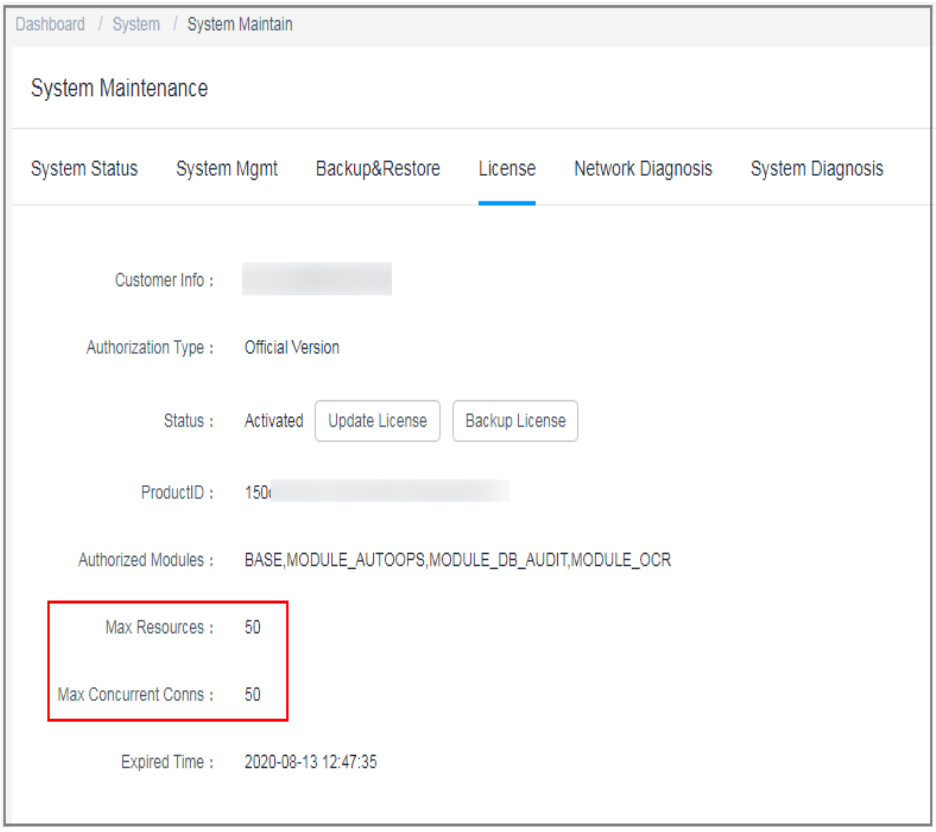
   NOTE

   The device system version must be V3.2.16.0 or later, or the change does not take effect. **Upgrade the system software** first if needed.

Step 3 Confirm and record the authorization configuration.

1. Choose **System** > **System Maintain** > **License** to view the authorization information.

Figure 1-3 Viewing license



2. Record the number of authorized resources in **Max Resources** and the number of concurrent connections of authorized resources in **Max Concurrent Conns**.

----End

1.2.2 Backing Up the CBH System Data

To prevent system data loss caused by possible change failures, back up important system data, including system configurations, resource accounts, and audit logs, before the change.

Backing Up System Configuration Data

You can back up CBH system configuration data and load it to the new CBH system, eliminating the need to repeat manual configurations.

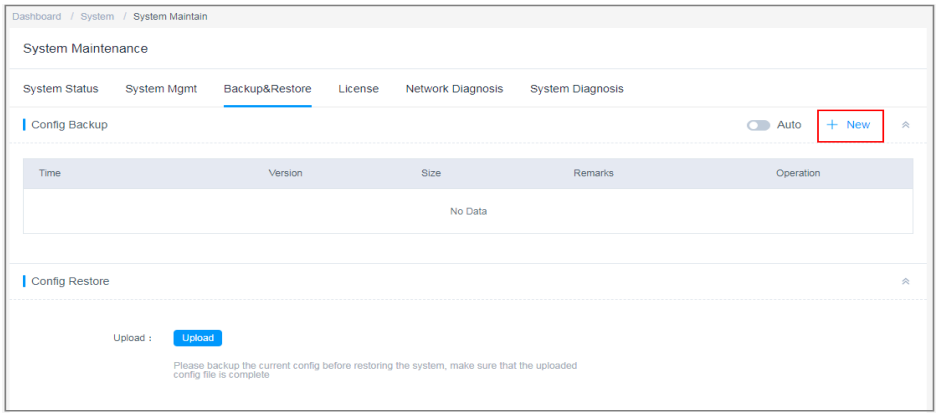
The system configuration data contains all configuration data of the department, user, resource, policy, ticket, operation, audit, and system modules.

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

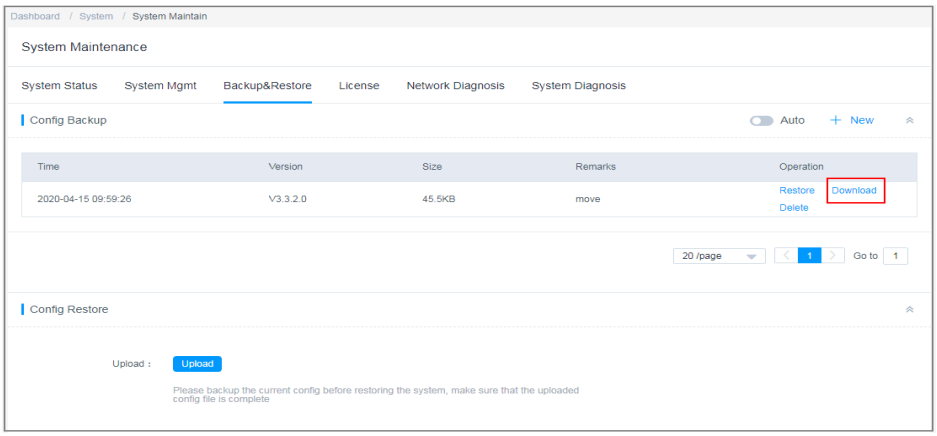
Step 3 Click **New** to back up the system configuration data.

Figure 1-4 Creating a configuration backup



Step 4 Click **Download** to export the system configuration file to a local computer.

Figure 1-5 Downloading a backup file



----End

Backing Up Managed Accounts

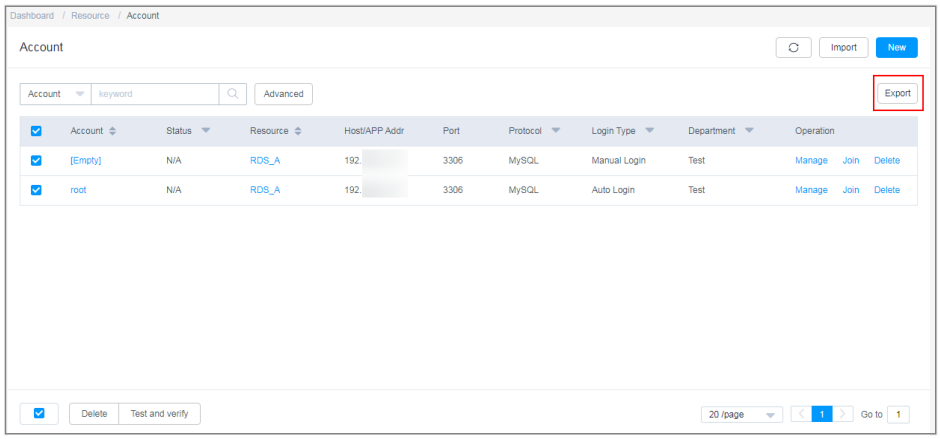
The authentication keys of different CBH systems are different. After the specification change, the managed accounts imported using the configuration file may fail to be used for system login. You are advised to back up managed accounts to prevent account information loss in case of specification change failure.

A managed account file contains all data of each account, including the username, password, login methods, sudo account, and names and addresses of associated resources.

Step 1 Log in to the CBH system.

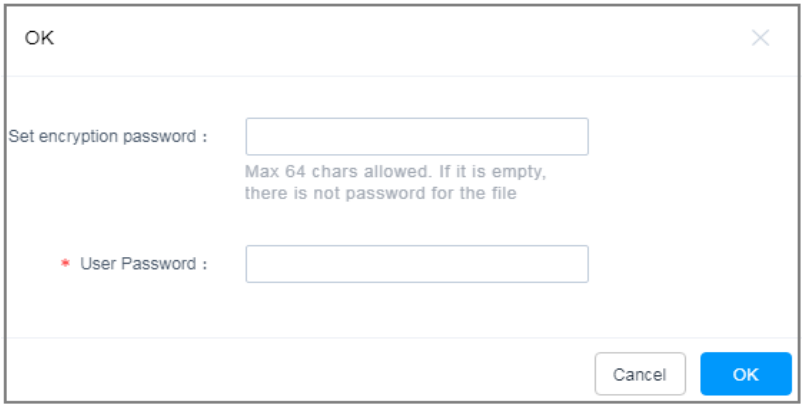
Step 2 Choose **Resource** > **Account** and click **Export**.

Figure 1-6 Exporting the account file



Step 3 Set the encryption password to encrypt the exported managed account file.

Figure 1-7 Setting encryption password



Step 4 Click **OK** and save the file locally.

----End

Backing Up Audit Logs

CBH does not support migration of history audit logs. You need to back up system audit logs before the change.

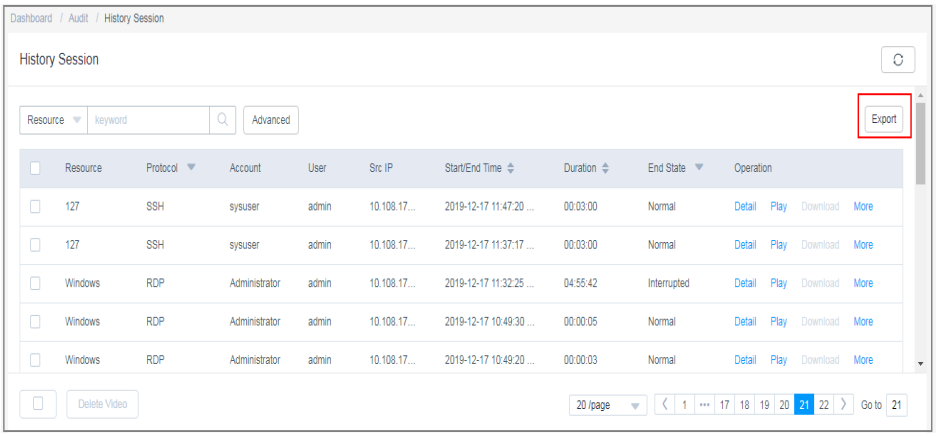
Audit logs include history session records, session videos, system login logs, system operation logs, password change logs, and account synchronization logs.

Step 1 Log in to the CBH system.

Step 2 Export history session records.

1. Choose **Audit** > **History Session**.
2. Select all history sessions, click **Export**, and save exported text records locally.

Figure 1-8 Exporting history session records



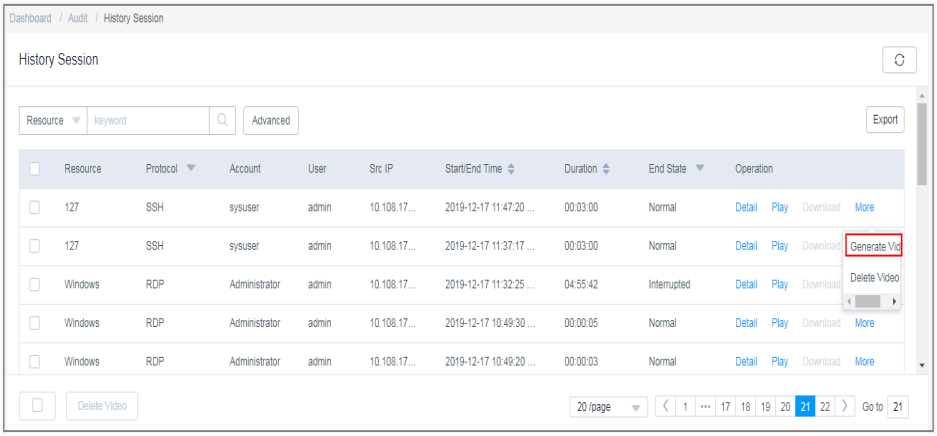
Step 3 Download a session video.

NOTE

Session videos cannot be generated or downloaded in batches. Only one video can be generated or downloaded at a time.

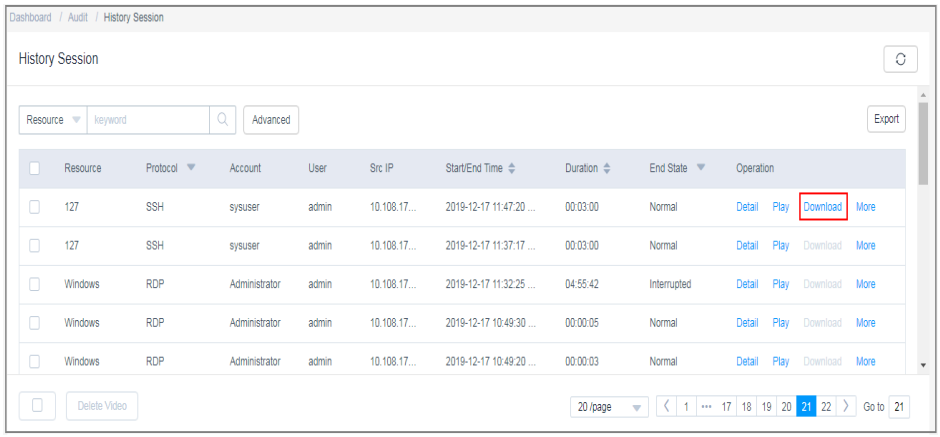
1. Choose **Audit** > **History Session**.
2. Choose **More** > **Generate Video** in the **Operation** column of the target session row.

Figure 1-9 Generating a video



3. After the video is generated, click **Download** and save the video locally.

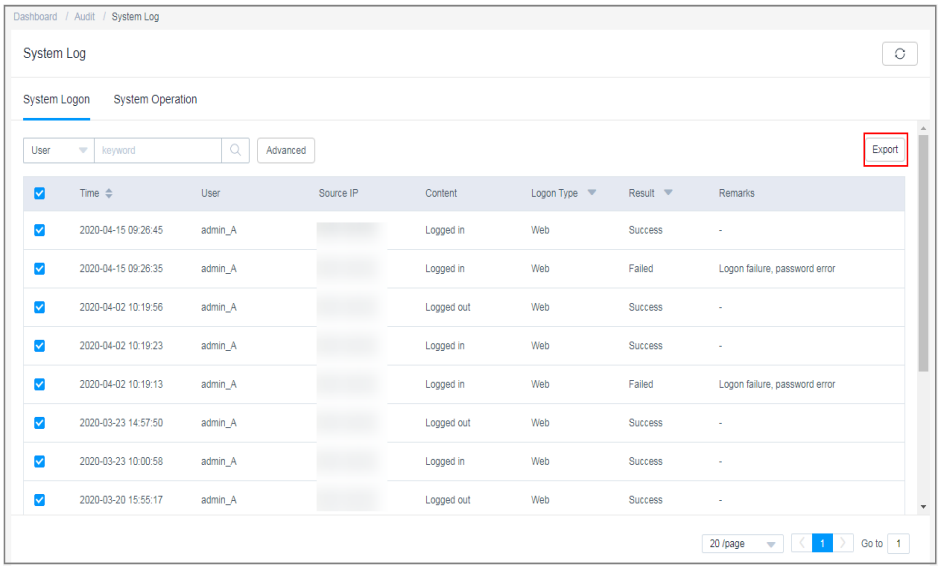
Figure 1-10 Downloading a video



Step 4 Export system login logs.

1. Choose **Audit** > **System Log** > **System Logon** to switch to the system log page.
2. Select all login logs, click **Export**, and save the exported text records locally.

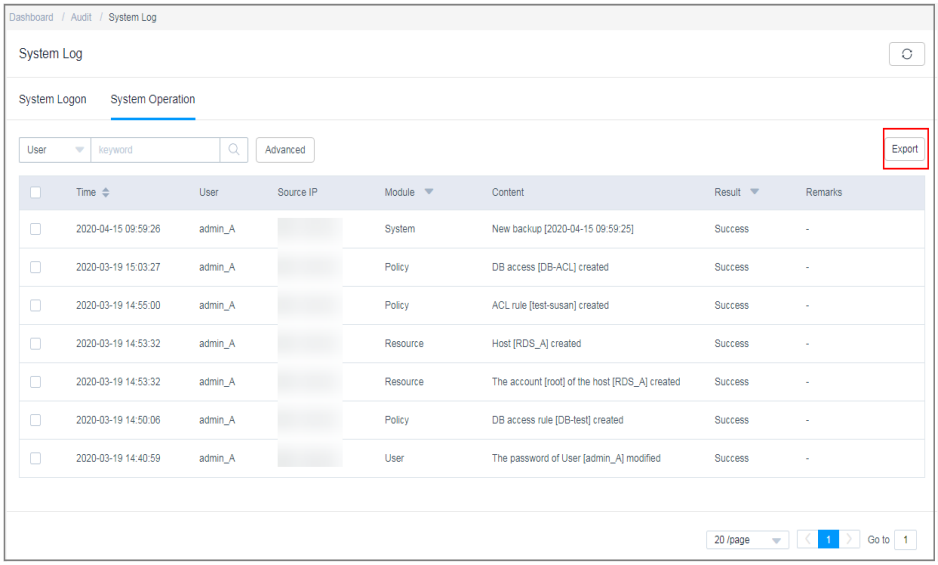
Figure 1-11 Exporting system login logs



Step 5 Export system operation logs.

1. Choose **Audit** > **System Log** > **System Operation** to switch to the system log page.
2. Select all operation logs, click **Export**, and save the exported text records locally.

Figure 1-12 Exporting system operation logs



----End

1.3 Changing Specifications of a CBH Instance

Prerequisites

- You have obtained credentials for logging in to the management console.
- An EIP has been bound to the CBH instance.
- You have backed up system data by referring to **Backing Up the CBH System Data**.
- You have disabled the CBH system and terminated all other operations in the CBH system.

Procedure

Step 1 Log in to the management console.

Step 2 In the **Operation** column of the target instance, choose **More** > **Change Edition**.

Figure 1-13 Instances

Step 3 Select an edition you want.

Select an **Edition** and click **Next** to go to the **Details** page.

Step 4 Confirm and pay the order.

After confirming the order details, click **Submit**. On the payment page, finish the payment.

Step 5 The specifications are automatically changed in the background.

It takes about 30 minutes for the change to take effect.

During the change, the instance status changes from **Upgrading** to **Restarting**. After the CBH system is restarted, the instance status changes to **Running**.

Step 6 The specifications are changed in the background.

If the instance status changes to **Running** and the instance details are updated, the backend change is completed.

You can then log in to the CBH system and start to verify the change.

----End

1.4 Verification After the Change

1.4.1 Checking the System Environment

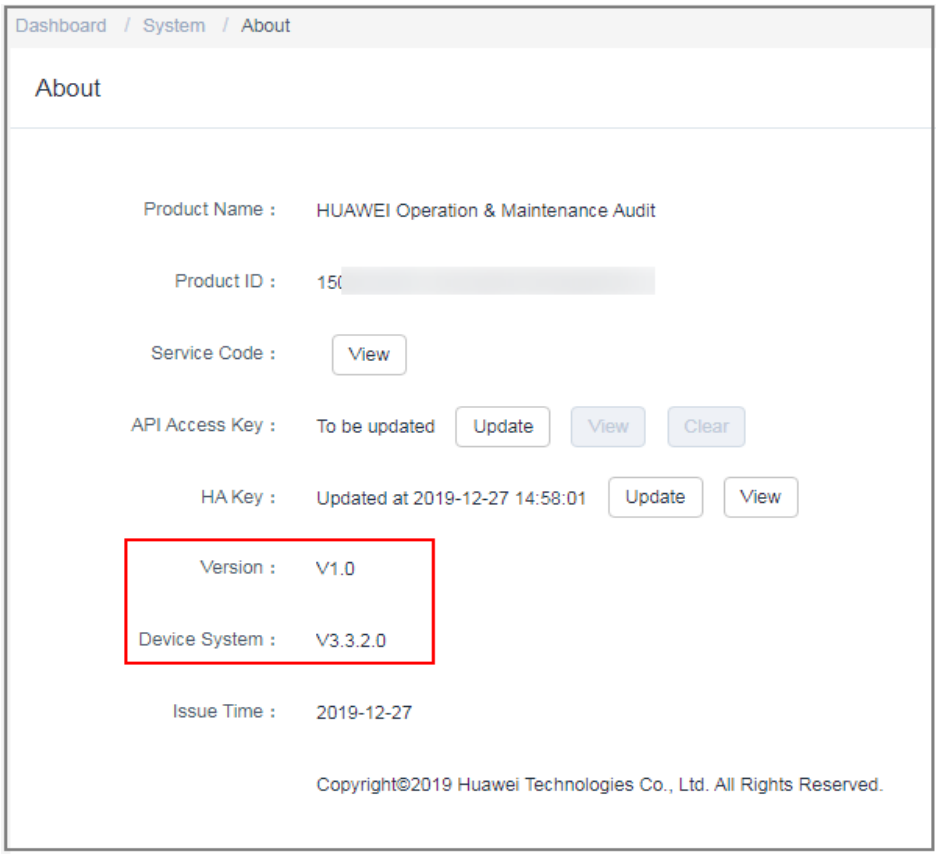
After the change, verify that the settings of **Version**, **Device System**, **Max Resources**, and **Max Concurrent Conns** are the same as that of the new CBH edition.

Step 1 Log in to the CBH system.

Step 2 Verify the system version.

1. In the navigation pane on the left, choose **System** > **About** to view the system version information.
2. Check the information of **Version** and **Device System**.

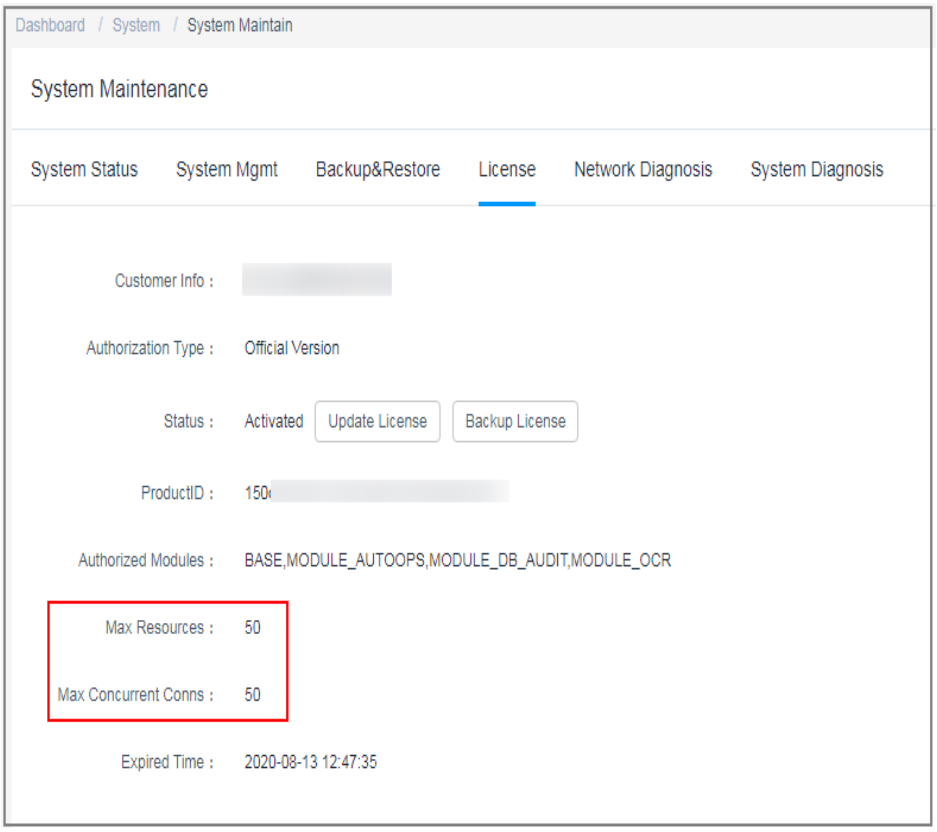
Figure 1-14 Viewing CBH system version number



Step 3 Check whether the original and new CBH systems have the consistent authorization information.

1. Choose **System** > **System Maintain** > **License** to view the authorization information.

Figure 1-15 Viewing license



2. Check whether the authorization information is consistent with that of the new CBH edition.
   - If they are consistent, the specification change is successful.
   - If no, contact technical support.

----End

1.4.2 (Optional) Restoring CBH System Configurations

After the change is completed, the number of system assets, number of concurrent requests, CPU, and data disks are upgraded accordingly, which does not affect system data.

If system data is lost due to a change failure, you can import the backup files, such as system configuration files and resource account files, and restore the system configurations.

Importing the Backup File of the CBH System Configurations

You can reuse the system configuration data of the original CBH system in the new CBH system by uploading the system configuration back file to the new system.

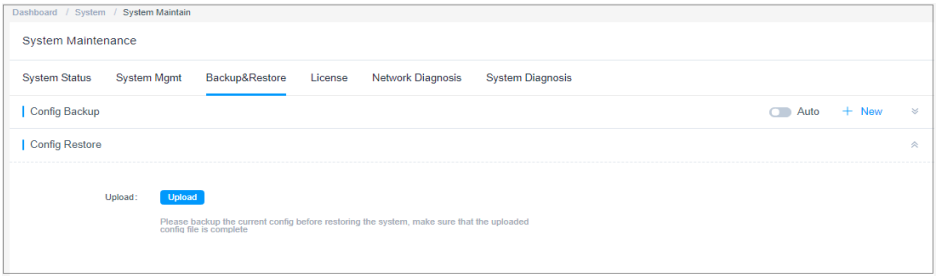
The system configuration data contains all configuration data of the department, user, resource, policy, ticket, operation, audit, and system modules.

Step 1 Log in to the CBH system.

Step 2 Choose **System** > **System Maintain** > **Backup&Restore**.

Step 3 In the **Config Restore** area, click **Upload**, select the configuration file exported from the original CBH system, and upload it.

Figure 1-16 Uploading the backup configuration file



Step 4 Click **OK**.

It takes about 5 minutes for the imported configuration data to take effect. It may take a longer time if there is a large amount of system configuration data.

----End

Importing the Backup File of Managed Accounts

The authentication keys of different CBH systems are different. After the change, the managed accounts imported using the configuration file may fail to be used for system login. To ensure the availability of the managed accounts, you are advised to import the backup file of the managed accounts.

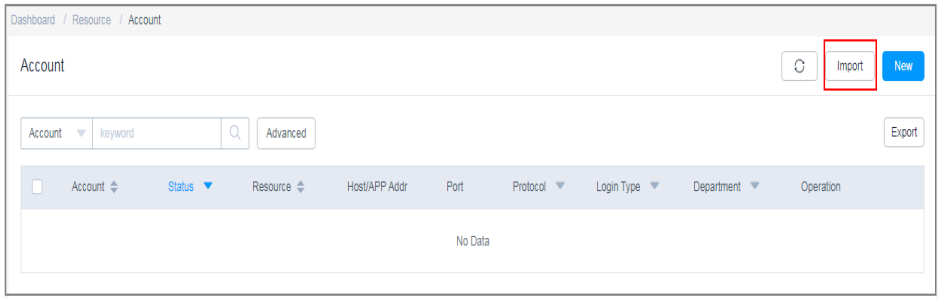
A managed account backup file contains all data of each account, including the username, password, login methods, sudo account, and names and addresses of associated resources.

Step 1 Log in to the CBH system.

Step 2 Choose **Resource** > **Account** in the navigation pane.

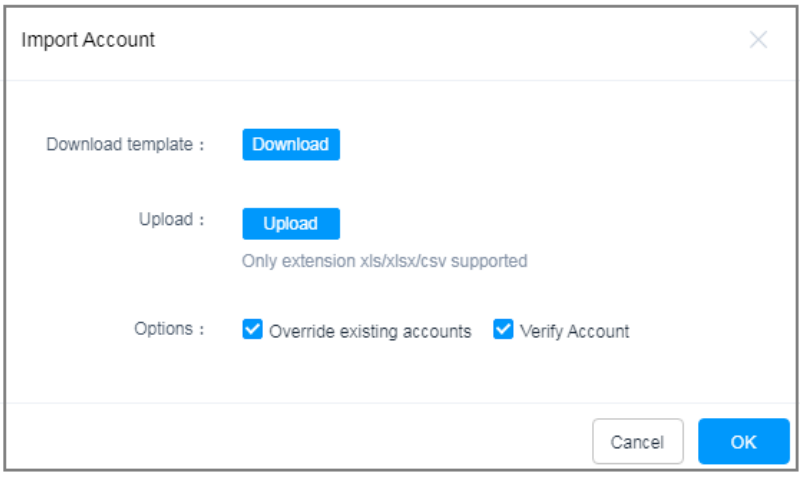
Step 3 Click **Import** to go to the **Import Account** page.

Figure 1-17 Account



Step 4 On the **Import Account** page, click **Upload**, select the account file exported from the original CBH system, and upload it.

Figure 1-18 Import Account



Step 5 After the upload is complete, choose **More** > **Override existing accounts** or **Verify Account**.

Step 6 Click **OK**.

----End

1.4.3 (Optional) Resetting the Passwords of System Users

After the specifications of a CBH instance are changed, you are advised to reset the system user passwords to enhance the password security and availability.

You can let the system generate a new password for users in batches or manually reset different passwords for system users.

Step 1 Log in to the CBH system.

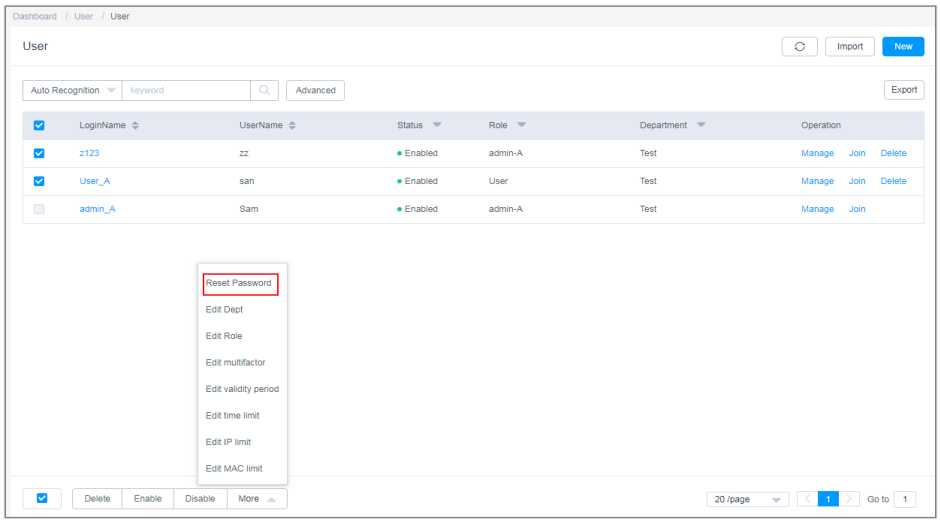
Step 2 Choose **User** > **User** in the navigation pane.

- To reset passwords in batches, go to **Step 3**.
- To manually reset a password, go to **Step 4**.

Step 3 Reset the same login password of multiple system users.

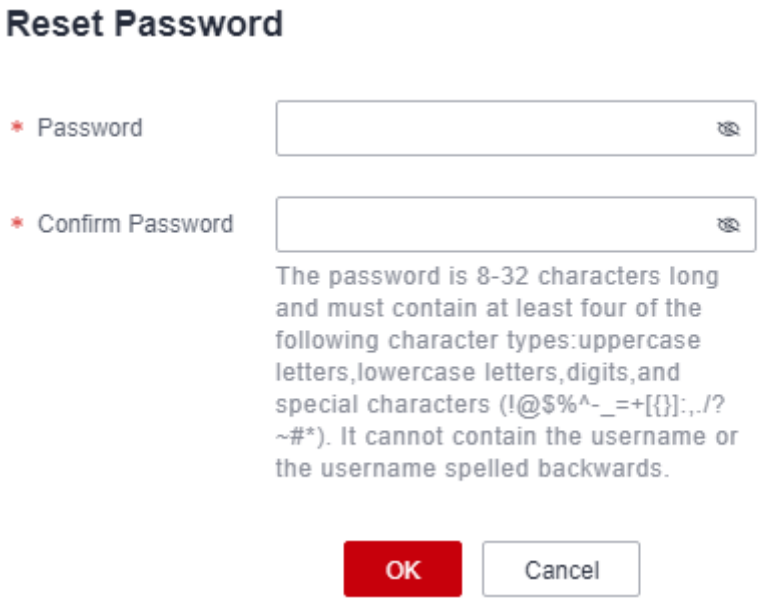
1. Select the users whose password needs to be reset.

Figure 1-19 Resetting a user's password



2. Choose **More** > **Reset Password** to go to the password resetting dialog box.

Figure 1-20 Reset Password



3. Reset the password and click **OK**.

NOTE

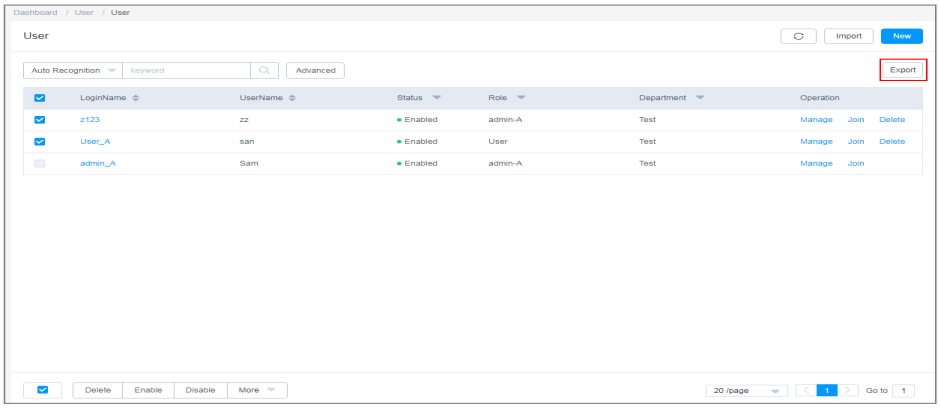
After you batch reset the passwords for multiple system users, these users need to use the reset password to log in to the CBH system. For security purposes, CBH asks each system user to change the password upon the first login.

Step 4 Manually reset different passwords for system users.

1. Export the user list template.

   Select the users you want to export and click **Export** in the upper right corner. If no users are selected, information about all users is exported by default.

Figure 1-21 Exporting information about all users



2. Configure user passwords.

   Save the exported user information file locally, change the plaintext password in the **Cleartext Password** row corresponding to the user **Login Name** as needed, and save the file.

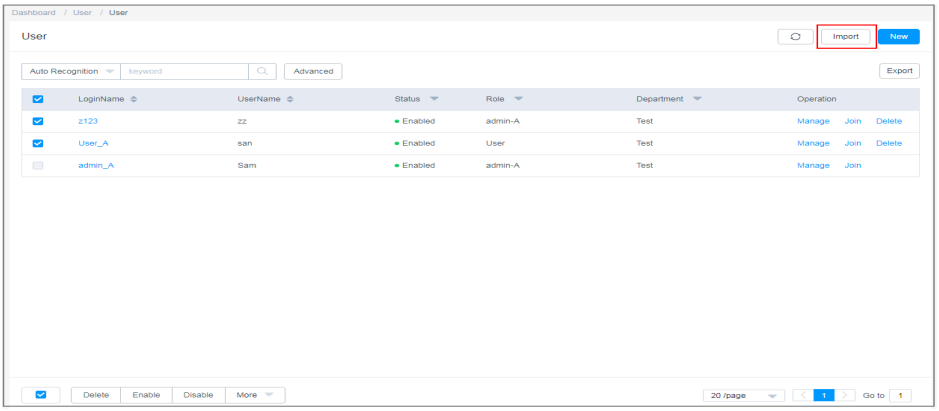
Figure 1-22 Changing a password

Login name	AuthType	Cleartext Password	AD domain	Username	Mobile	Email	Role	Dept	Remarks	User Group
User_A	Local	29fHLTx!3c$\		san	134****922	te****@hu	User	Test		G2
z123	Local	/^c~8Mn6NO1p		zz	124****9224	te****@hu	admin-A	Test		

3. Import the user list.

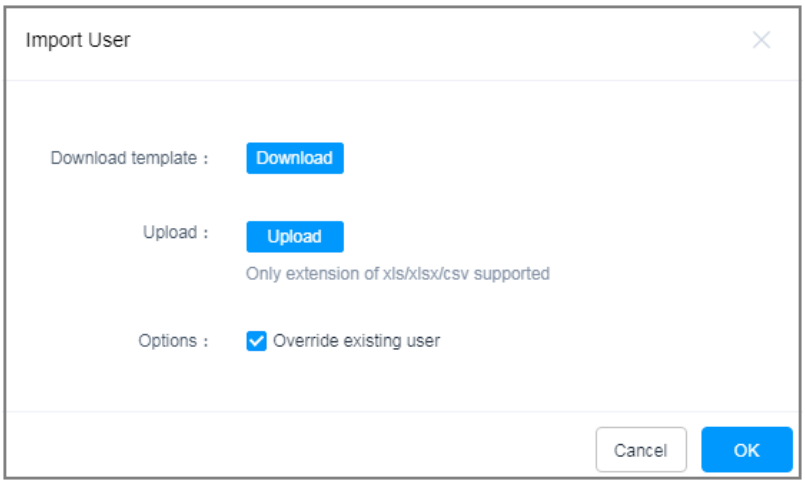
   a. On the **User** page, click **Import**.

   Figure 1-23 Importing the user information file



   b. Click **Upload** and select the modified user information file.

Figure 1-24 Import User



c. Select **Override existing user** for **Options**.

d. Click **OK**.

----End

1.4.4 Verifying the CBH System configurations

After the instance specifications are changed, log in the CBH system as system administrator **admin** to verify system configuration consistence for each module in the navigation pane of the CBH system.

You need to verify system configurations in the department, user, resource, policy, ticket, audit, operation, and system modules. For more details, see **Table 1-2**

Table 1-2 System configuration verification

Level 1 Module	Level 2/3 Module	Verification Item
Department	None	Department level, department name, number of users, and number of hosts.
User	User	Number of users and basic information about each user, such as the login name, user name, status, role, and department.
	User Group	Number of user groups, user group names, and group members.
	Role	Role configuration.
Resource	Host	Number of managed hosts and basic information about each managed host, including the host name, host address, port number, protocol type, OS type, and number of accounts.

Level 1 Module	Level 2/3 Module	Verification Item
	Application Publish	• Number of applications, names, addresses, associated hosts, and department of each application. • Number of application servers, names, addresses, types, and department of each application server.
	Account	• Number of accounts and basic information about each account, including the account name, related resources, host or application address, port number, and department. • Whether accounts can be used. You can select accounts in batches and click **Verify** to check whether the selected accounts can be used to log in to the system.
	Account Group	Number of account groups, account group names, members in an account group, and number of members in an account group.
Operation	Host label	Number of labels of managed hosts, such as the number of labels, names, and labeled hosts.
	Application Label	Verify the configuration information about the number of tags, names, and tagged application resources released by the application.
Policy	ACL Rules	Number of ACL rules and basic information about each ACL rule, such as rule name, status, associated users, and associated accounts.
	Cmd Rules	• Number of policies, policy names, actions, and associated command sets. • Number of command sets, names, commands, and parameters.
	Chpwd Rules	Number of policies and basic information about each policy, such as policy names, status, execution modes, and password change mode.
Audit	System Report	**Auto Send** configuration
	Ops Report	**Auto Send** configuration
Ticket	ACL Ticket	Basic information about the authorization ticket, including ticket number, status, and application time
System	Security	System login security configuration, including user locking, policy password, web login, and SSH client login.

Level 1 Module	Level 2/3 Module	Verification Item
	Outgoing	Email and SMS gateway configuration.
	Authenticate	AD domain, RADIUS, and LDAP authentication configurations.
	Ticket	Basic settings and approval process of tickets.
	Alarm	Alarm channel and alarm level (severity)
	Storage Mgmt	Auto deletion.
	Log Backup	Remote backup to the Syslog server and remote backup to the FTP/SFTP server.
	Backup& Restore	Automatic configuration backups.

2 Secondary Authorization for High-Risk Database Operations

With CBH editions, you can delete, modify, and view your database instances by running commands. To secure sensitive database information and prevent key information from being lost or disclosed, CBH gives you the ability to configure an approval process for high-risk database operations and monitor key information.

Use administrator ***admin_A*** as an example to describe how to authorize O&M user ***User_A*** to perform secondary authorization for high-risk operations on MySQL database instance ***RDS_A***.

Application Scenarios

With Cloud Bastion Host (CBH), you can dynamically identify and intercept high-risk commands (including deleting databases, modifying key information, and viewing sensitive information) to interrupt database O&M sessions by setting database control policies and preset command execution policies. In addition, the system automatically generates a database authorization ticket and sends it to the administrator for secondary authorization. O&M users can resume interrupted O&M sessions only after the administrator approves the ticket and authorizes the high-risk operations.

Constraints

Currently, secondary authorization of high-risk operations only applies to the commands executed on the MySQL or Oracle database instances.

Prerequisites

- The security group to which the CBH instance belongs has enabled the database access port, and the network connection between the database and the CBH system is normal.
- Database ***RDS_A*** has been managed as a host resource.
- O&M user ***User_A*** has obtained the access control permission for ***RDS_A***.

Configuring the Secondary Authorization Policy

To approve high-risk operations on database instances, you need to preset command rules on the **DB Rules** page in the **Policy** module and enable **Dynamic approval** in the **Action** field.

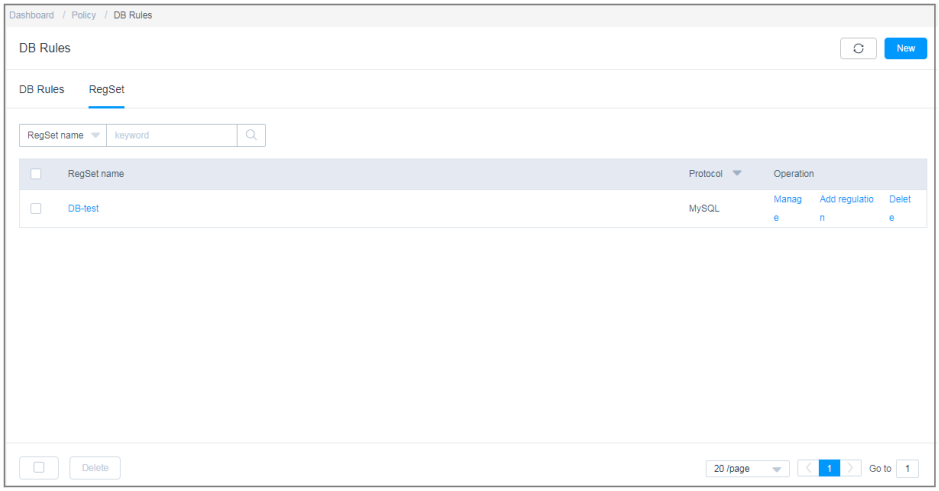
Step 1 Log in to the CBH system as ***admin_A***.

Step 2 Choose **Policy** > **DB Rules** to go to the **DB Rules** page.

Step 3 Configure the database rule set and select the preset high-risk operation commands.

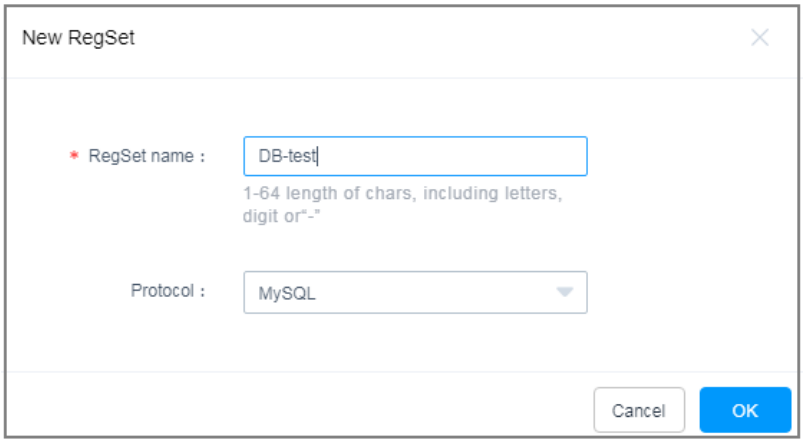
1. Click the **RegSet** tab.

Figure 2-1 RegSet



2. Click **New** to create a rule set for MySQL databases. Use the ***DB-test*** rule set as an example.

Figure 2-2 New RegSet

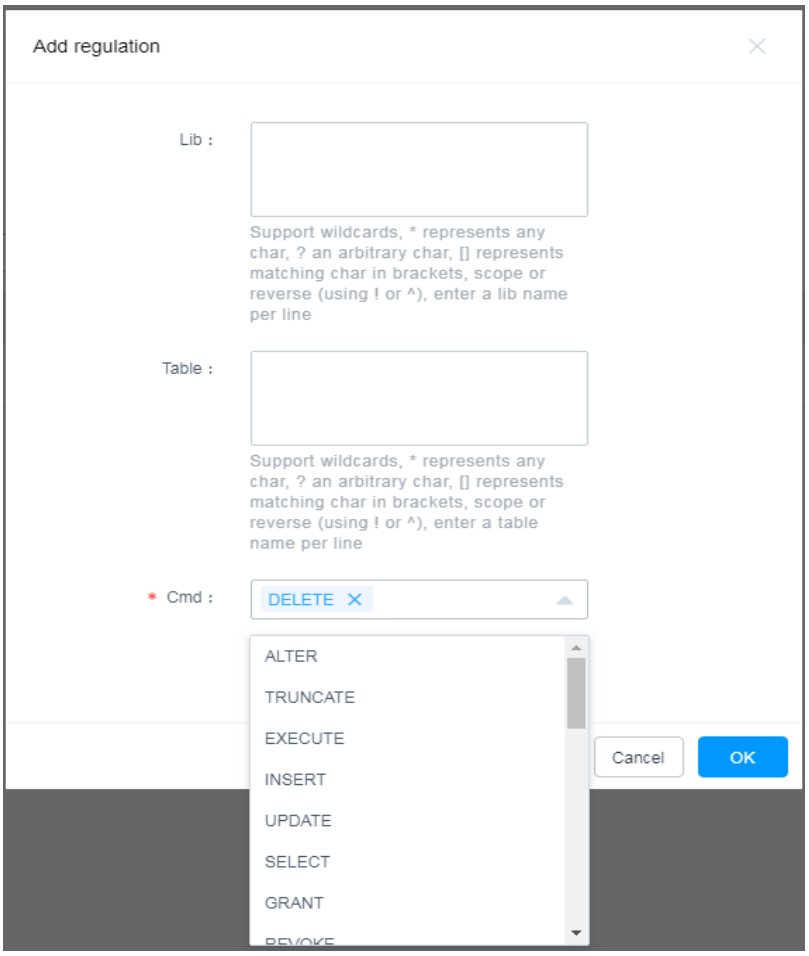


3. Click **Add Regulation** in the **Operation** column of the ***DB-test*** row to add a library, table, or command rule. The following describes how to add the **DELETE** command for deleting table content.

NOTE

- The **Cmd** field is mandatory. You must select at least one command. You can select multiple commands at a time.
- Set the **Lib** or **Table** field to restrict operation commands on the database library or tables.
- If the **Lib** or **Table** field is left blank, all operation commands in the database are restricted.

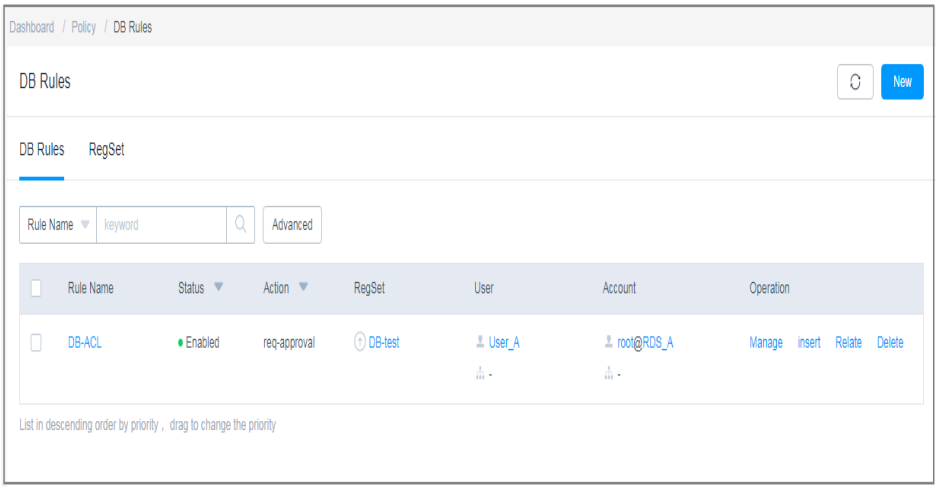
Figure 2-3 Add regulation



Step 4 Configure a DB rule.

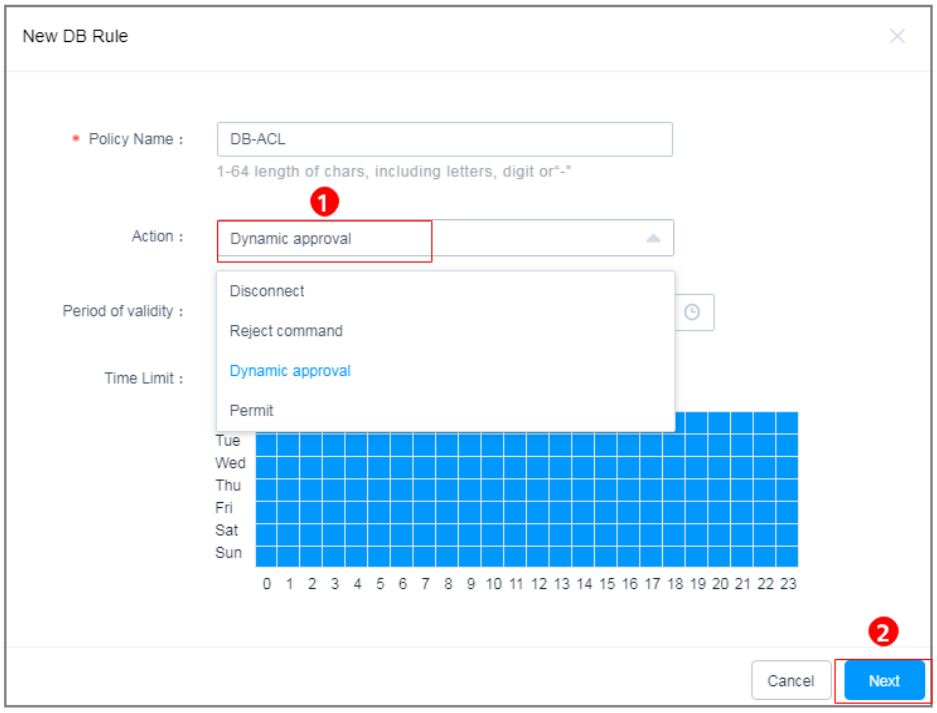
1. Click the **DB Rules** tab.

Figure 2-4 DB Rules



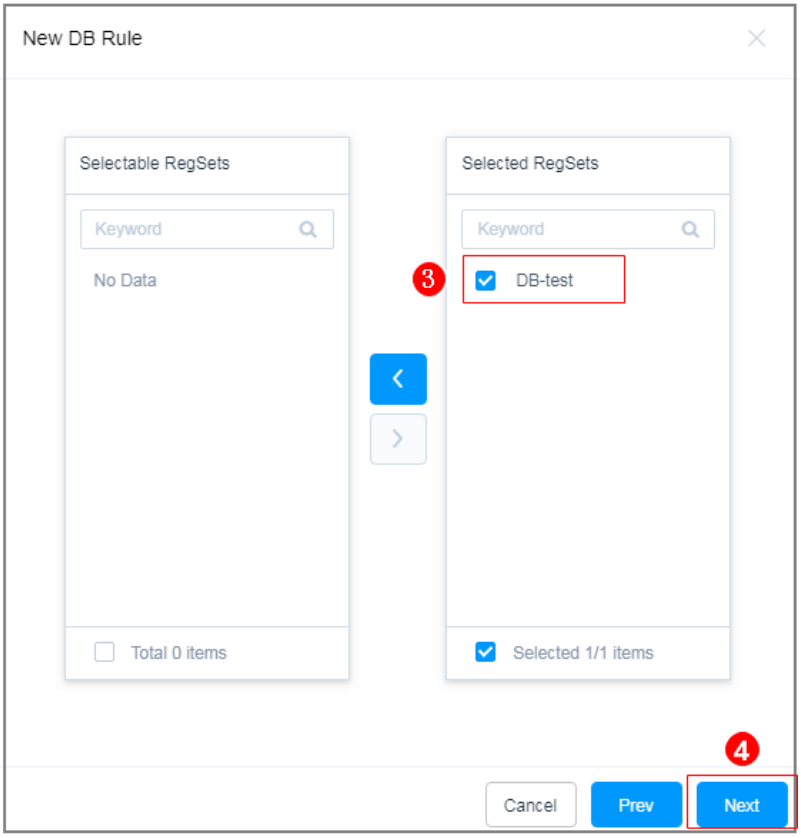
2. Click **New** to create a **Dynamic approval** rule for the database. Use database rule ***DB-ACL*** as an example.

Figure 2-5 Configuring dynamic approval



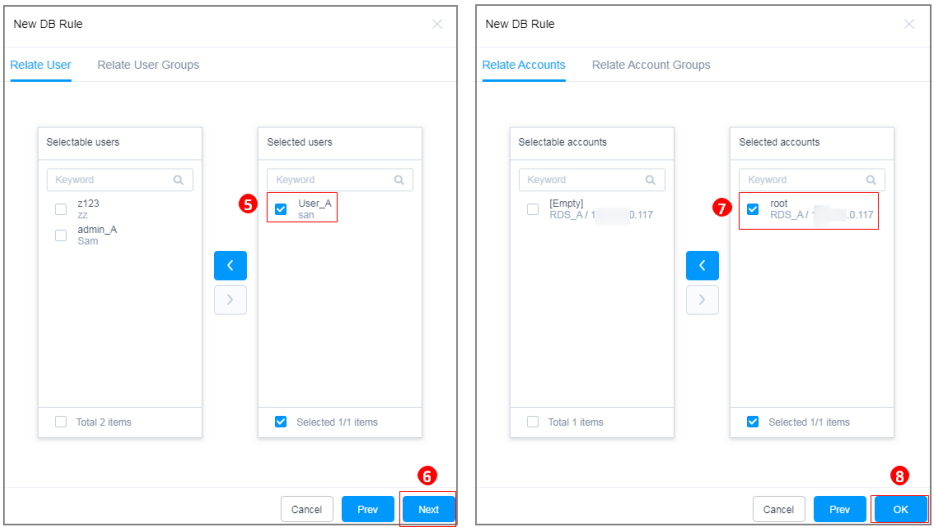
3. Relate the rule to rule set ***DB-test***.

Figure 2-6 Relating a new database rule to a rule set (RegSet)



4. Relate user ***User_A*** to resource ***RDS_A***.

Figure 2-7 Relating users to resources



----End

Verifying the Secondary Authorization Policy

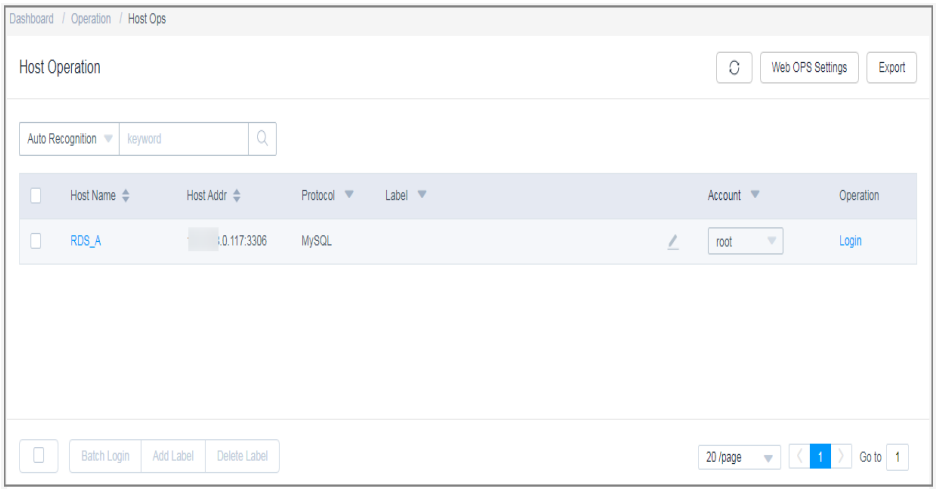
An O&M user performs a high-risk operation and applies for operation permissions after the operation is intercepted. The administrator authorizes the

high-risk operation after review to strengthen the management and control of core database assets.

Step 1 Log in to ***RDS_A*** as O&M user ***User_A***.

1. Log in to the CBH system.
2. Choose **Operation** > **Host Ops**.
3. Click **Log In** to log in to database resource ***RDS_A*** using an SSO tool.

Figure 2-8 Database login

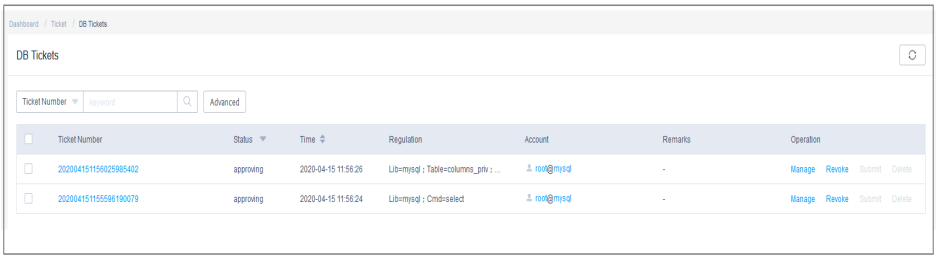


Step 2 Use the Navicat client as an example. O&M user ***User_A*** deletes table content from ***RDS_A***. The **DELETE** command is automatically intercepted, and a message is displayed indicating that ***User_A*** does not have the permission to delete the table content.

Step 3 O&M user ***User_A*** submits a database authorization ticket to administrator ***admin_A*** for approval of the deletion operation.

1. Log in to the CBH system as O&M user ***User_A***.
2. Choose **Ticket** > **DB Tickets** and view the tickets generated due to the interception of the deletion.
3. Click **Submit** to submit the application for granting the required permissions on ***RDS_A***.

Figure 2-9 DB Tickets



Step 4 The ***admin_A*** approves or rejects the O&M operations performed by ***User_A*** based on situation.

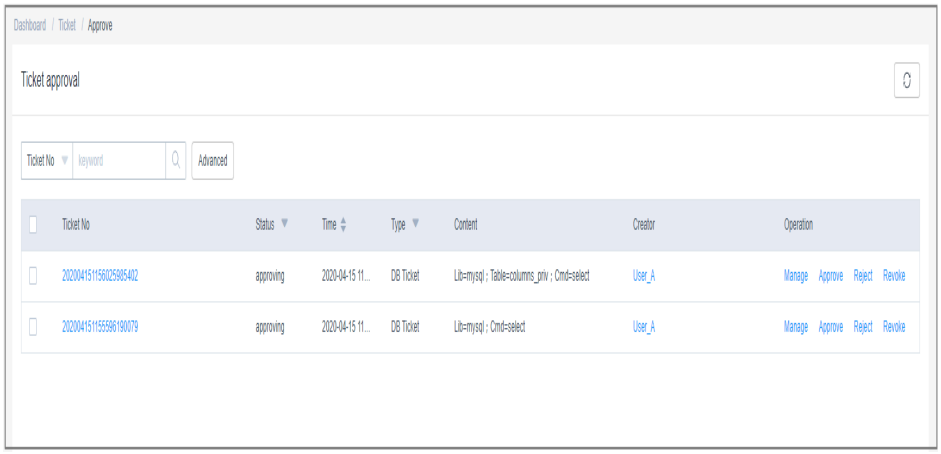
1. Log in to the CBH system as administrator ***admin_A***.

2. Choose **Ticket** > **Approve** and review the ticket submitted by ***User_A***.
3. Click **Approve** or **Reject** to approve or reject the ticket.

   NOTE

   Only after the administrator approves the ticket, the O&M user can resume the intercepted high-risk operations.

Figure 2-10 Ticket approval



----End

3 CBH for DJCP (or MLPS)

This topic describes which CBH functions are useful for DJCP certification. So that you can use certain functions and provide supporting materials accordingly to win DJCP certification easily.

Articles Related to DJCP Level 3 Certification

The following part focuses on the following DJCP articles:

- Security audit should be performed on network borders and important network nodes. Every user's critical behaviors and security events shall be audited.
- Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.
- Audit records shall be protected and backed up periodically to avoid unexpected deletion, modification, or overwriting.
- Behavior audit and analyses shall be separately performed for remote access user behaviors and Internet access user behaviors.
- The identity of the login user shall be identified and authenticated. The ID shall be unique, and the identity authentication information shall meet complexity requirements and be changed periodically.
- Response measures to login failures, including stopping sessions, restricting the number of illegal logins, and automatically logging off expired network connections, shall be configured and enabled.
- During remote management, necessary measures shall be taken to prevent authentication information from being intercepted during transmission.
- Two or more authentication methods, including tokens, passwords, and biometric technologies, shall be used to authenticate user identity. Password authentication must be used.
- Appropriate accounts and permissions shall be assigned to login users.
- Default accounts shall be renamed or deleted, and their passwords should be changed.
- Redundant or expired accounts should be deleted or disabled in time to avoid account sharing.
- The minimum permissions shall be granted to management users to implement separation of privilege.

- Access control policies should be configured by the authorization subject, and the access policy should specify the rules for the subject to access the authorized object.
- The security audit function must be provided for each user to audit important security incidents and user behavior.
- Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.

Prerequisites

You have purchased a later bastion host of the standard edition or later and completed the bastion host configuration.

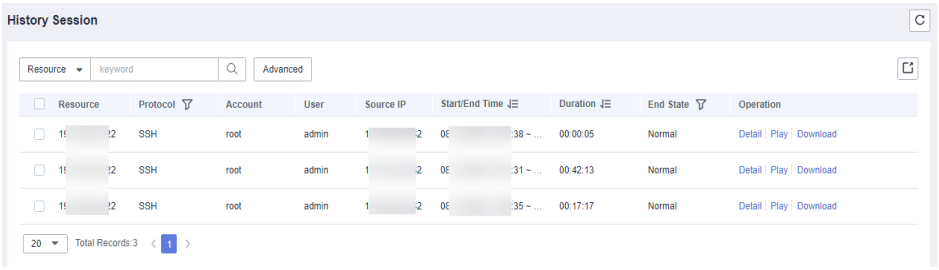
Security Zone Border: Security Audits

- DJCP article: **Security audit should be performed on network borders and important network nodes. Every user's critical behaviors and security events shall be audited.**

  This clause focuses on whether security audit is performed. CBH supports monitoring and security audits for O&M activities on cloud servers.

  - Log in to the CBH system using an account with the permission on the audit module. Choose **Audit** > **History Session**.

    Figure 3-1 Viewing historical sessions

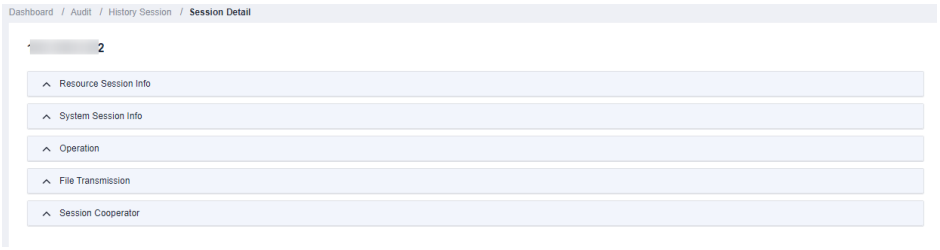
    

  - On the history session page, you can view resource session information, system session information, operation records, file transmission records, and collaborative session records.
- DJCP article: Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.

  This article checks whether logs are recorded as required.

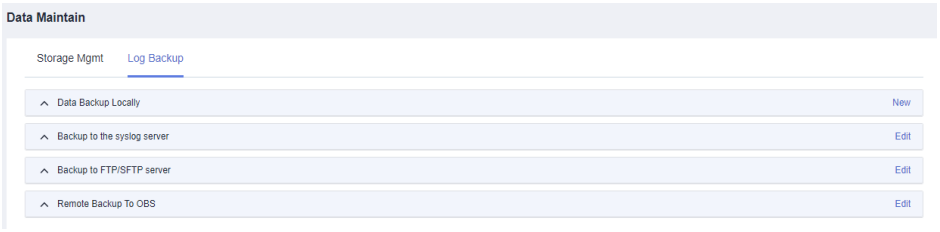
  - Log in to the CBH system using the administrator account. Choose **Audit** > **History Session**.
  - For a history session, you can view the resource name, type, host IP address, account, start and end time, session duration, session size, operation user, source IP address and MAC address of the operation user, login mode, operation records, file transfer records, and session collaboration records.

Figure 3-2 Viewing historical sessions



- Audit records shall be protected and backed up periodically to avoid unexpected deletion, modification, or overwriting.
  - Log in to the CBH system as the administrator, choose **System > Data Maintain**, and click **Log Backup** to go to the **Log Backup** page.
  - On the **Log Backup** page, you can create and view log backups, including system login logs, resource login logs, command operation logs, file operation logs, and two-person authorization logs. Data can also be backed up to the Syslog server, FTP server, SFTP server, and an OBS bucket.

Figure 3-3 Creating a database backup



- Behavior audit and analyses shall be separately performed for remote access user behaviors and Internet access user behaviors.

  This article checks whether remote access user activities and log data can be audited and analyzed.

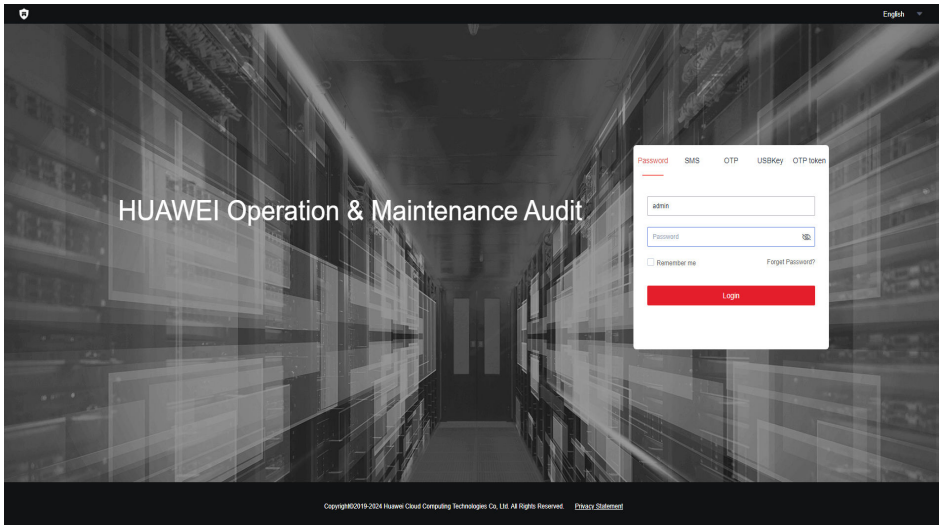
Secure Computing Environment: Identity Authentication

- DJCP article: The identity of the login user shall be identified and authenticated. The ID shall be unique, and the identity authentication information shall meet complexity requirements and be changed periodically.

  This clause focuses on the following three points:

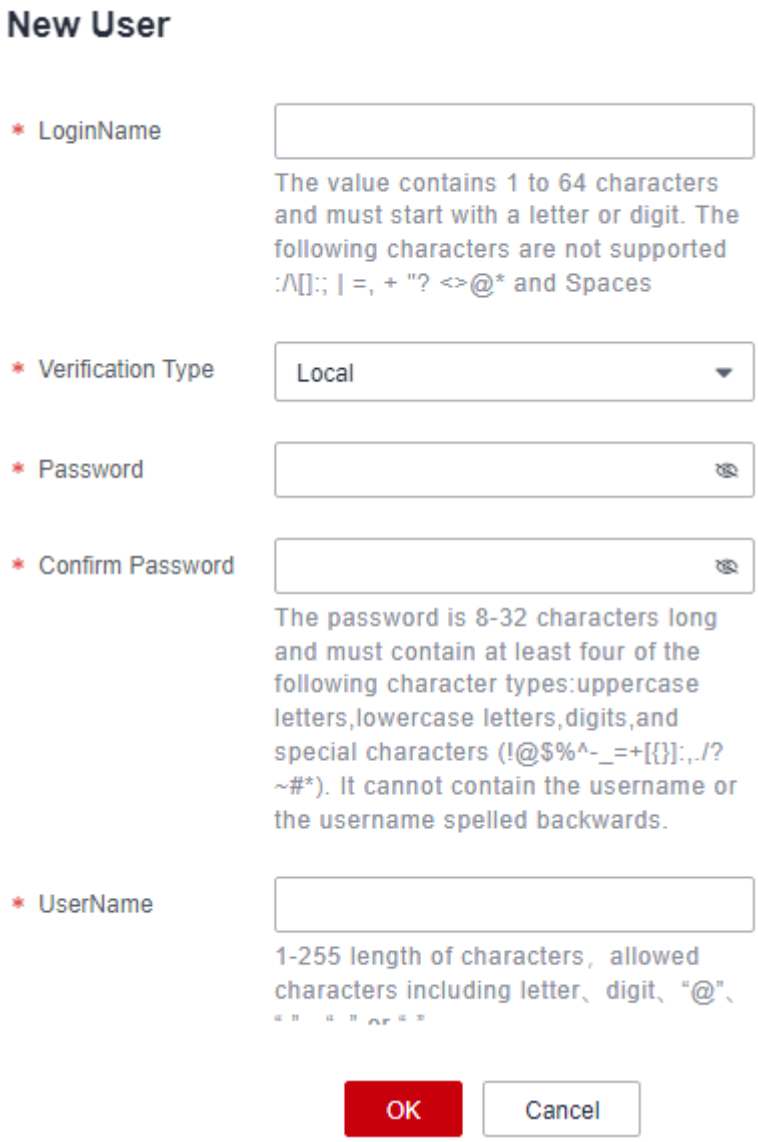
  a. Check whether the login user is identified and authenticated. If the user accesses the bastion host page using a browser, the product functions can be used only after the user identity is authenticated.

Figure 3-4 CBH system login page



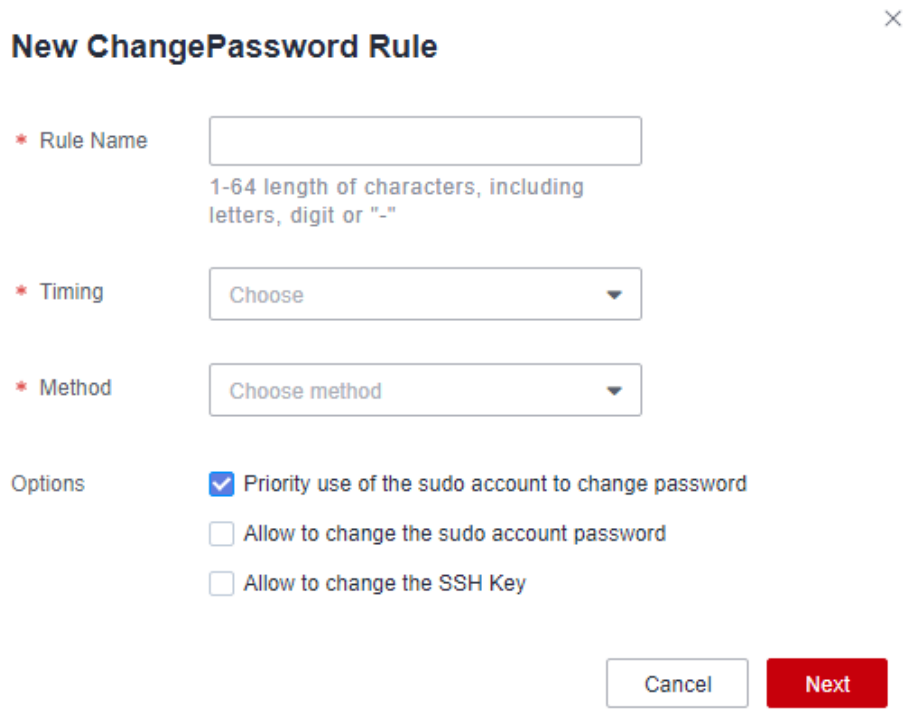
b. Uniqueness: When creating users, the username, mobile number, email address, and role must be unique for each user. Only one role can be configured for a user. For details, see **Creating a CBH System User**.

Figure 3-5 Creating a user



c. Check whether password complexity and periodic change requirements on identity authentication are met. CBH supports manual, scheduled, and periodic password change methods. In addition, CBH supports generating different passwords, generating the same password, and specifying the same password for quickly change passwords for system users. For details, see **CBH Password Change Rules**.

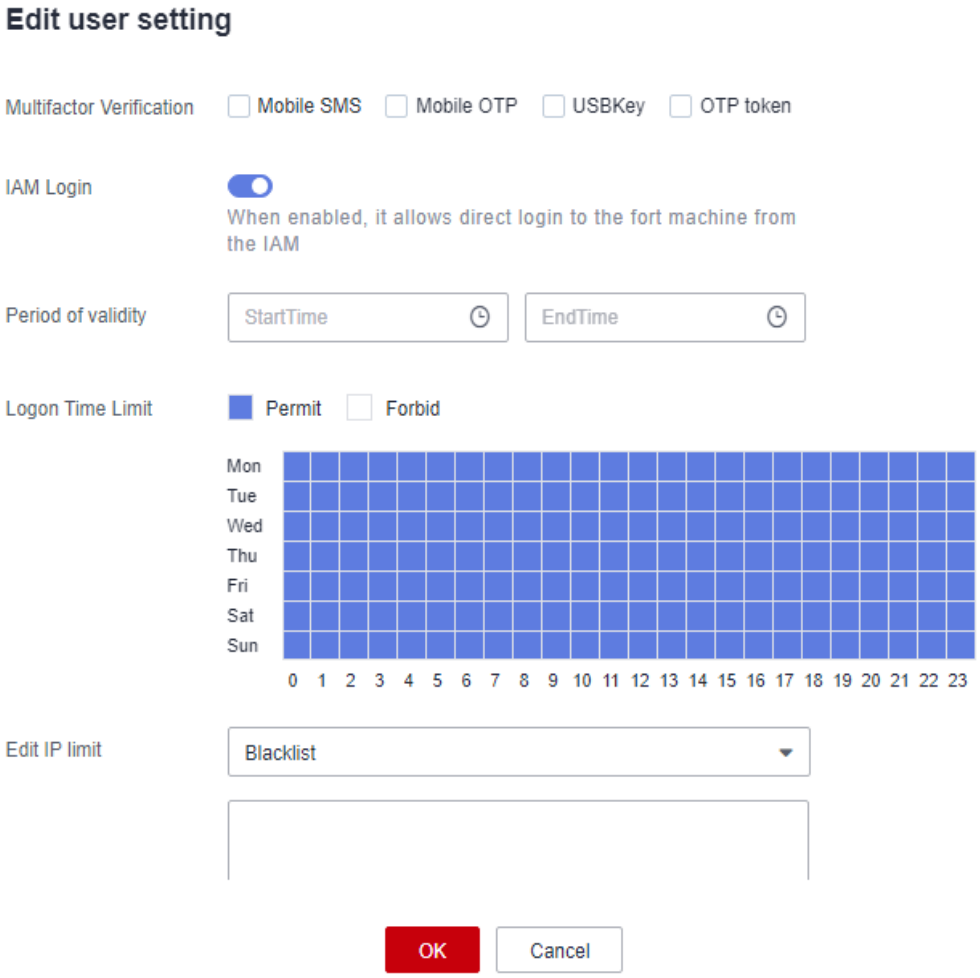
Figure 3-6 Chpwd Rules



- DJCP article: Two or more authentication methods, including tokens, passwords, and biometric technologies, shall be used to authenticate user identity. Password authentication must be used.

  CBH uses multi-factor authentication. The login authentication methods include SMS messages, mobile phone tokens, USB keys, and dynamic OTPs.

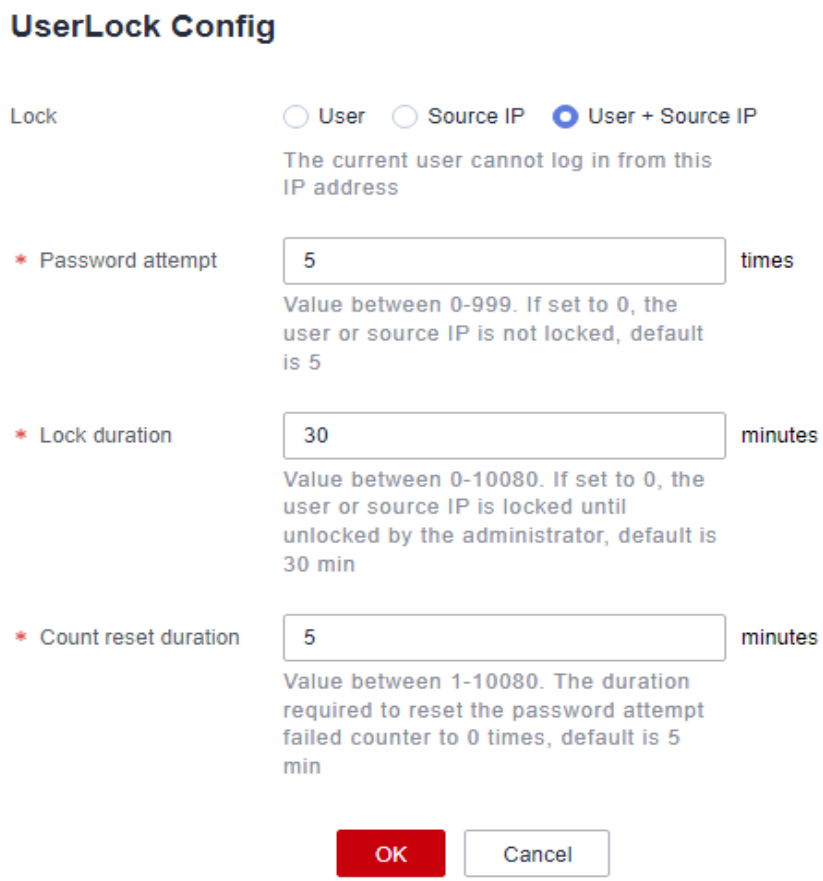
Figure 3-7 Configuring Multifactor Verification



- DJCP article: Response measures to login failures, including stopping sessions, restricting the number of illegal logins, and automatically logging off expired network connections, shall be configured and enabled.

  You can configure a security lock for user login, including the lock mode, lock duration, and maximum number of password attempts.

Figure 3-8 User login lockout



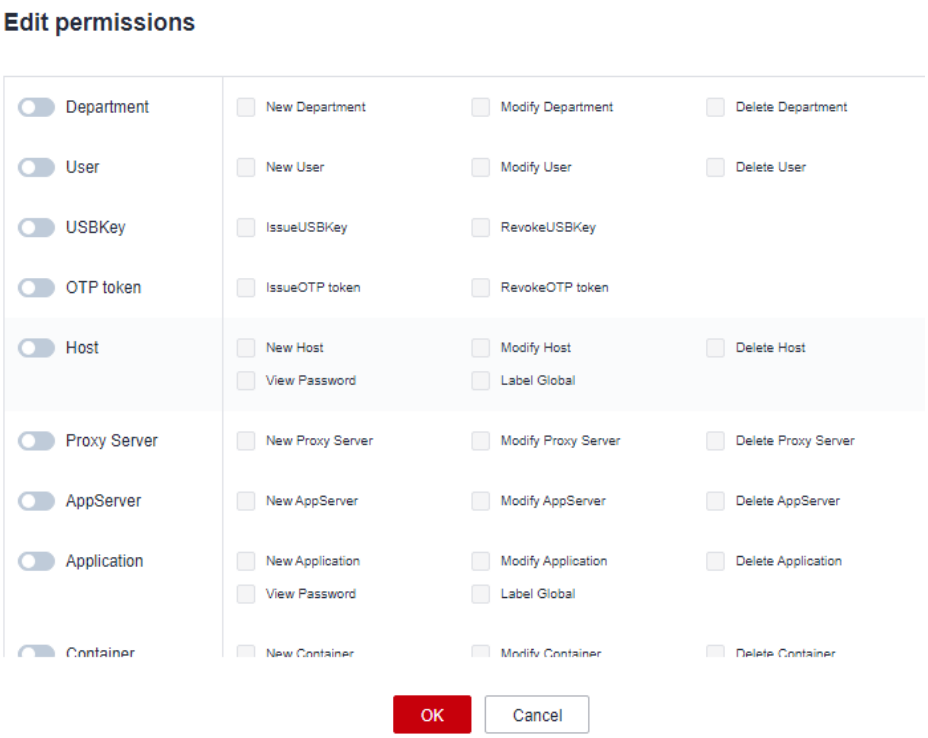
Access Control

- DJCP article: The minimum permissions shall be granted to management users to implement separation of privilege.

  CBH supports three types of user operation permissions: access control, command control, and database control policies.

  a. CBH can control some operation permissions based on login user roles. For example, you can grant the permission to delete and modify proxy servers to the O&M manager account.

Figure 3-9 Fine-grained role permissions



b. You can control access to specific functions, such file management, upstream clipboard, downstream clipboard, watermark display, login time control, file upload, and file download. You can also allow or block the users of certain source IP addresses to access managed resources.

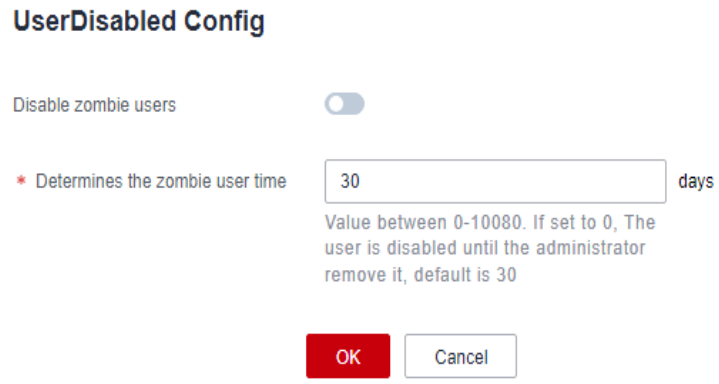
Figure 3-10 ACL Rules

- DJCP article: Appropriate accounts and permissions shall be assigned to login users.

  CBH allows you to assign roles to users and create user groups for users. For details, see *User Role Management* and *CBH User Group Management* in the *Cloud Bastion Host User Guide*.

  Accounts that have not been used for a long time or have expired should be deleted in a timely manner. You can set a validity period for each CBH system user. Once the validity period expires, the corresponding account will be disabled as a zombie user.

Figure 3-11 Zombie user identification rule



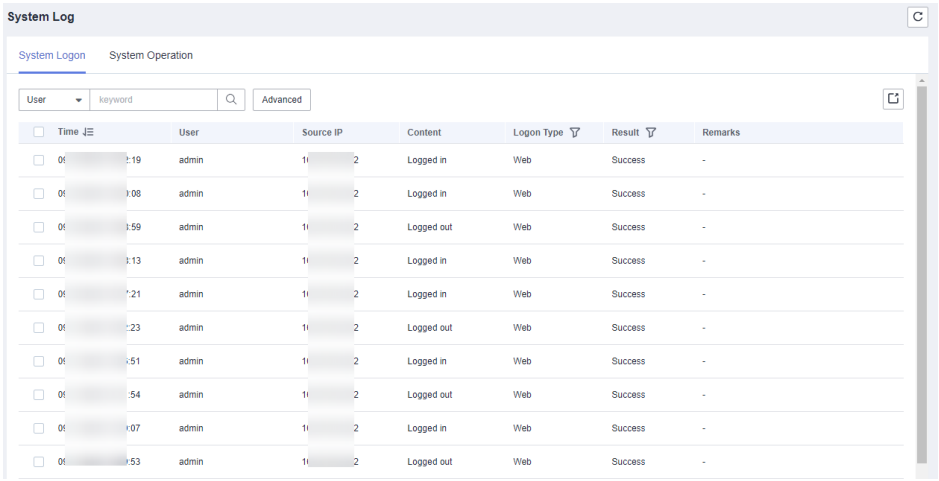
Security Audits

- DJCP article: The security audit function must be provided for each user to audit important security incidents and user behavior.

  CBH allows you to view real-time sessions, historical sessions, and system logs.

  You can view system login logs, including the login time, login user, source IP address, log content, login mode, login result, and remarks.

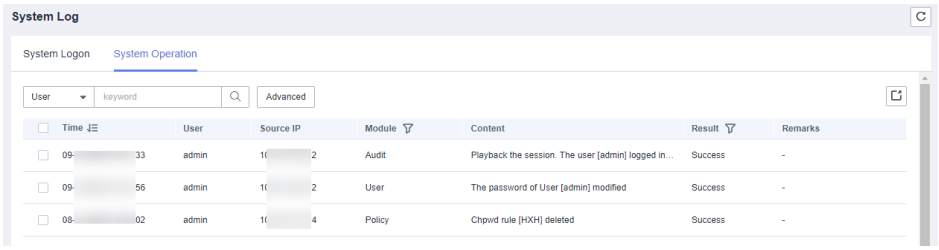
  Figure 3-12 System logon logs

- DJCP article: Audit records shall include the event date and time, users, event types, whether the events succeeded, and other related audit information.

  You can view which accounts performed what operations in system operation logs, including the user, time, source IP address, module, log content, and result.

  Figure 3-13 System operation logs

4 Cross-Cloud, Cross-VPC O&M for Resources On and Off the Cloud

Application Scenarios

If you have servers deployed across VPCs, in on-premises data centers, and across multiple clouds, CBH is always a good choice for centralized O&M. With CBH, you can manage scattered servers centrally without establishing dedicated lines, making O&M of all workloads efficiently and securely.

This topic describes how to use the CBH system to manage and maintain your resources across VPCs, clouds, and on-premises environments. Before doing this, you need to enable communications between your CBH instance and the network where the resources to be managed with CBH locate. The following walks you through how to configure a proxy server in a target network and connect the proxy server to a CBH system.

Prerequisites and Preparations

- Your CBH instance is running properly.
- You have purchased an ECS, and the ECS is running properly.
- You have obtained a server from the peer network domain as the proxy server.
- An EIP has been bound to the proxy server. For details, see **Binding an EIP to an Instance**.
- The proxy server can communicate with the servers you want CBH to manage.
- You have downloaded **the latest version 3proxy** package.

Setting the Proxy Server

Before managing and maintaining servers across network domains, you need to configure a network proxy server in the peer network domain. Then connect the proxy server to service servers through the intranet, and connect the proxy server to the CBH network. In this way, the CBH system can communicate with the service servers across domains.

This operation is the prerequisite for a bastion host to manage host resources across networks.

- **Enabling the Network Proxy Service for the Proxy Server**

Step 1 Log in to the proxy server and set the proxy server (assume it is named **3proxy**).

> **CAUTION**
>
> Commands in Step 2 to Step 4 are examples for CentOS 7. For details about example commands for CentOS 8, see **Example for Configuring a Proxy for CentOS 8**.

Step 2 Upload and decompress the 3proxy package, go to the corresponding directory, and run the following command:

bash install.sh

Step 3 Enter the following command to add the **3proxy** user:

/etc/3proxy/add3proxyuser.sh myuser mypassword

Step 4 Restart the proxy service **3proxy**.

systemctl restart 3proxy

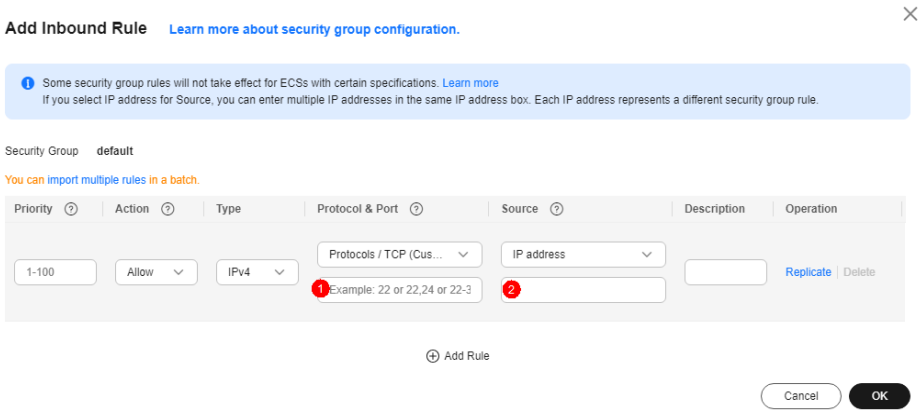
> **NOTE**
>
> - The SOCKS5 proxy protocol (port: 1080) does not provide the encryption function. If an unencrypted protocol is used for O&M through the proxy server, disable access from unnecessary IP addresses in the security group settings.
> - If encrypted transmission or data security is required, you can select an encrypted protocol when selecting an inbound or outbound rule. The protocol can be SSH, RDP, SFTP, SCP, or Rlogin.

----End

- **Configuring Security Group Rules for the Proxy Server**

Step 1 Configure **inbound rules** to allow the bastion host to access the proxy server.

Figure 4-1 Inbound rule configuration

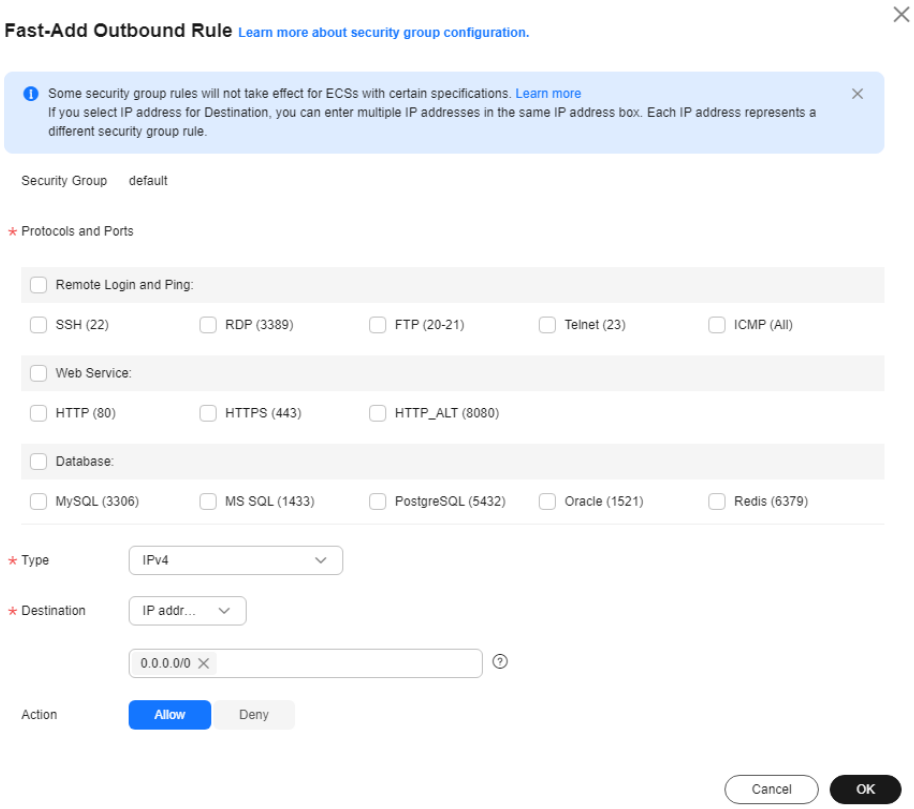


NOTE

- Set **Protocol & Port** to the default port **1080** for the SOCKS5 proxy server.
- Enter the IP address of the bastion host in the **Source** text box.

Step 2 Configure **outbound rules** for the proxy server to allow the proxy server to access the service servers managed with CBH.

Figure 4-2 Outbound rule configuration



----End

Using CBH to Manage Cross-Domain Service Servers

Step 1 Log in to the network console and choose **Access Control** > **Security Groups**. On the **Security Groups** page, configure the inbound and outbound rules of the security group associated with the CBH instance.

Figure 4-3 Configuring an inbound rule for a CBH instance

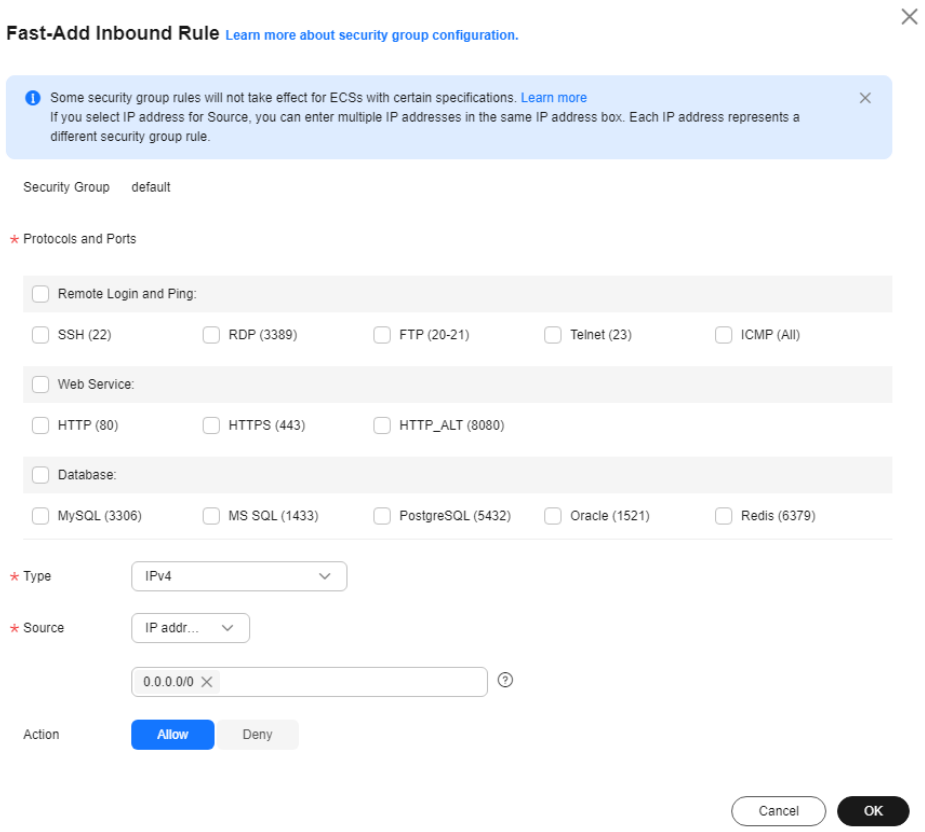
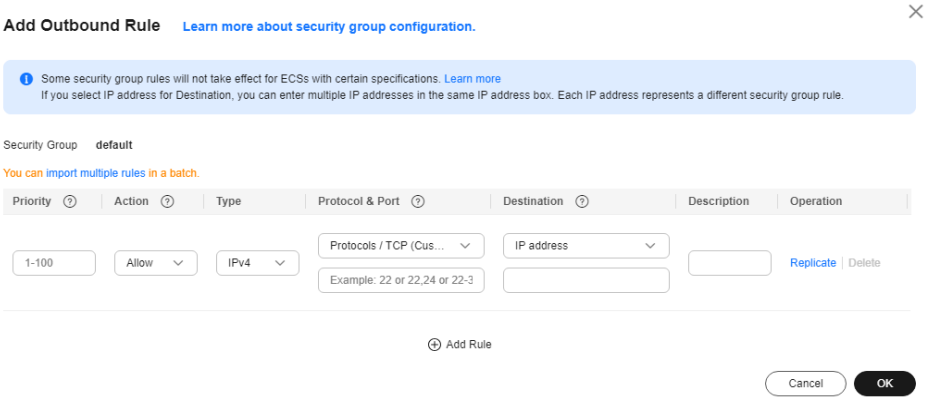
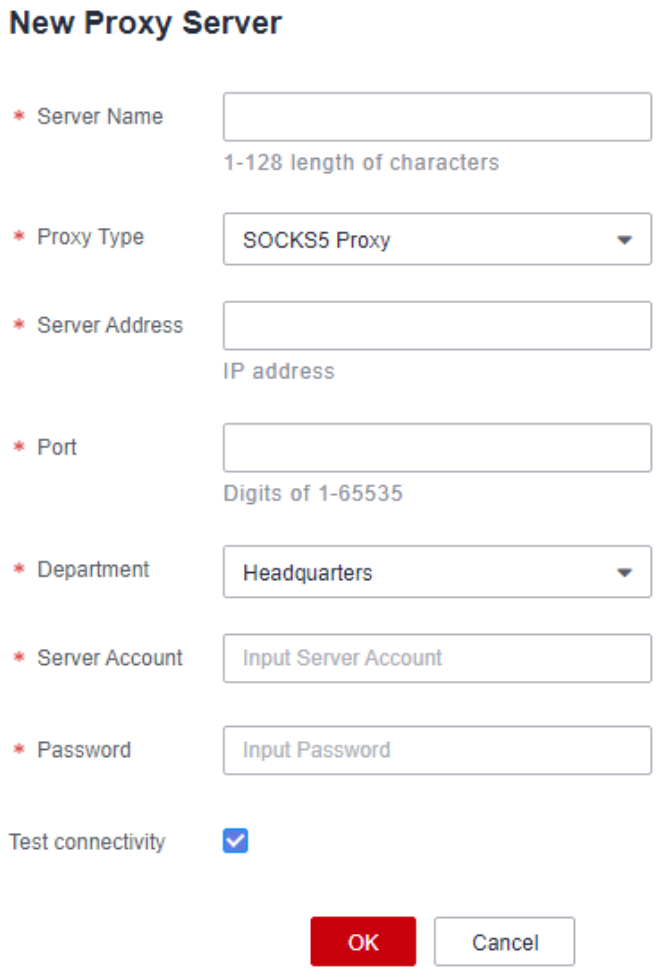


Figure 4-4 Configuring an outbound rule for a CBH instance



Step 2 Use CBH to manage proxy servers. Log in to the CBH system and add the proxy server. For details, see **Adding a Host**. On the **Host** page, click the **Proxy Server** tab and then **New**.

Figure 4-5 New Proxy Server



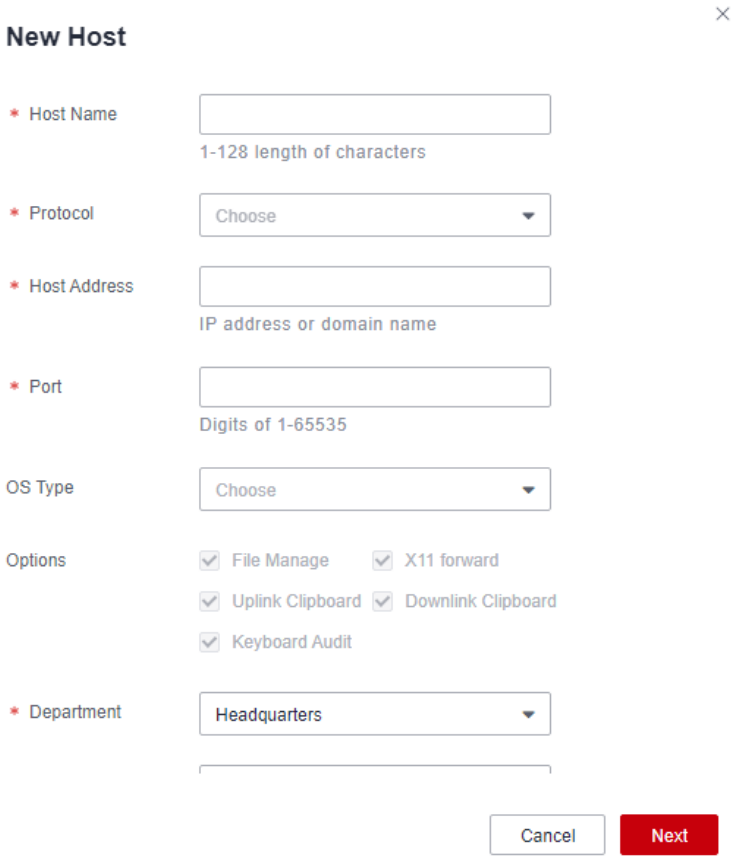
Step 3 Go back to the security group (the one you select in **Step 1**) your service servers belong to. On the **Inbound Rules** tab, click **Fast-Add Rule**.

NOTE

You can also add some outbound rules as required.

Step 4 Use CBH to manage service servers. For details, see **Adding Hosts**.

Figure 4-6 New Host



----End

After the preceding operations are performed, you can perform O&M on the managed hosts across network domains using the host operation function in CBH. Similarly, the preceding methods can be applied to different network environments such as hybrid/heterogeneous clouds and offline IDCs to implement unified online and offline O&M across clouds and VPCs.

Example for Configuring a Proxy for CentOS 8

Step 1 Run the following command to install the 3proxy software package:

yum install -y epel-release

yum install -y 3proxy

Step 2 Run the following command to perform simplified configuration:

nscache 65536

timeouts 1 5 30 60 180 1800 15 60

Set the username. Enter the username after the **users** command. Enter the username after the **CL** command. This section uses **test** as an example.

users test:CL:test

daemon

log /var/log/3proxy/3proxy.log

logformat "- +_L%t.%. %N.%p %E %U %C:%c %R:%r %O %I %h %T"

archiver gz /bin/gzip %F

rotate 30

external 0.0.0.0

internal 0.0.0.0

auth strong

allow test

maxconn 20

socks

flush

Step 3 Start the service.

systemctl start 3proxy

----End

5 How Can We Use CBH to Locate Incident Causes?

As cloud services develop, the number of cloud O&M engineers increases. In this case, security incidents may occur due to negligence. Tradition servers do not provide functions such as command monitoring and operation playback, resulting in incomplete traceability of security events.

CBH can manage and control all operations and log all operations in detail. Audit logs of sessions can be viewed online, recorded and played online, and played offline after being downloaded. CBH allows you to audit operations performed over character protocols (SSH and TELNET), graphics protocol (RDP and VNC), file transfer protocols (FTP, SFTP, and SCP), and database protocols (DB2, MySQL, Oracle, and SQL Server), as well as application publishing. For operations over character and database protocols, their operation instructions can be parsed so that you can know what actions have been done. For file transfer actions, the name and destination path of a transferred file can be logged.

Overview

This topic describes how to use CBH session audit function to trace and investigate security events and determine responsibilities.

Prerequisites

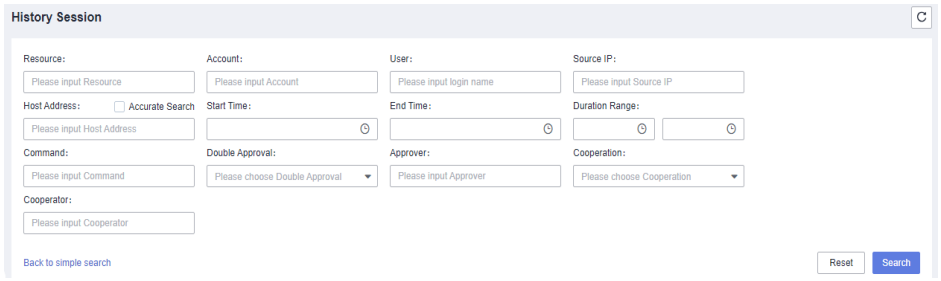
You have purchased a CBH instance and logged in to it using an account that has the audit module permission.

Auditing Historical Sessions

Step 1 Log in to CBH console. Go to the **History Session** page. For details, see **Viewing History Sessions**.

Step 2 Enter the related information in the advanced search box based on your security issues.

Figure 5-1 Advanced search



Step 3 Locate the target security issue, click **Detail** in the **Operation** column to view the historical commands and file transfers.

----End

You can locate the fault based on the commands, ensuring event traceability. You can also use the session playback function to view the specific operations by playing the corresponding O&M video. For details, see **Managing Session Videos**.

NOTICE

CBH also provides real-time session monitoring. This means you can view the O&M page of high-risk operations in real time. If an alarm is reported for an on-going risky command, the corresponding operations can be immediately terminated to ensure service security.

